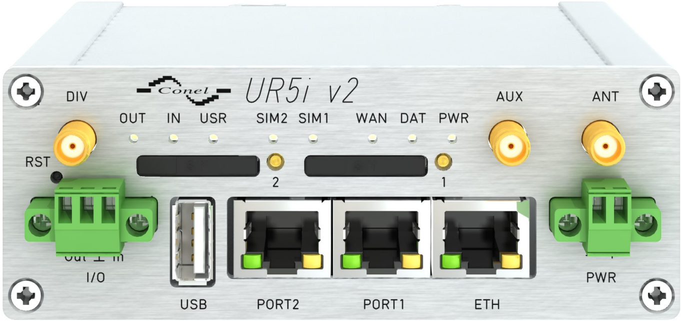
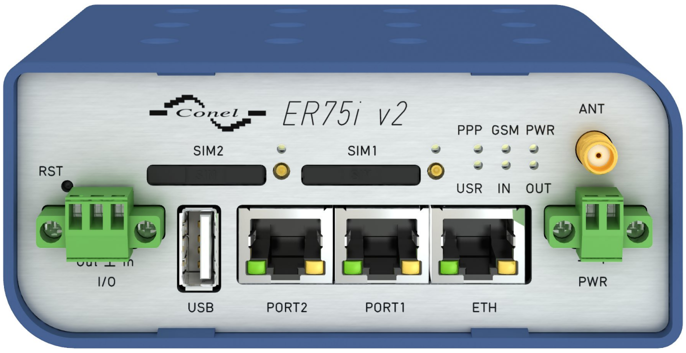
A B&B ELECTRONICS Company

The connecting & monitoring company

CONFIGURATION MANUAL

for v2 routers





Used symbols

⚠ *Danger* – important notice, which may have an influence on the user's safety or the function of the device.

❗ *Attention* – notice on possible problems, which can arise in specific cases.

ℹ *Information, notice* – information, which contains useful advice or special interest.

Firmware version

Actual version of firmware is 3.0.7 (12.7.2013).

GPL licence

Source codes under GPL licence are available free of charge by sending an email to:

info@conel.cz.

Router version

Properties and settings of router associated with the GSM connection is not available in industrial router XR5i v2.

PPPoE configuration item is only available on the industrial router XR5i v2, used to set the PPPoE connection over Ethernet.

CE

TÜVRheinland® COTI ISO 9001

Conel s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Manual issued in CZ, July 15, 2013

Contents

List of Figures

List of Tables

1. Configuration over web browser

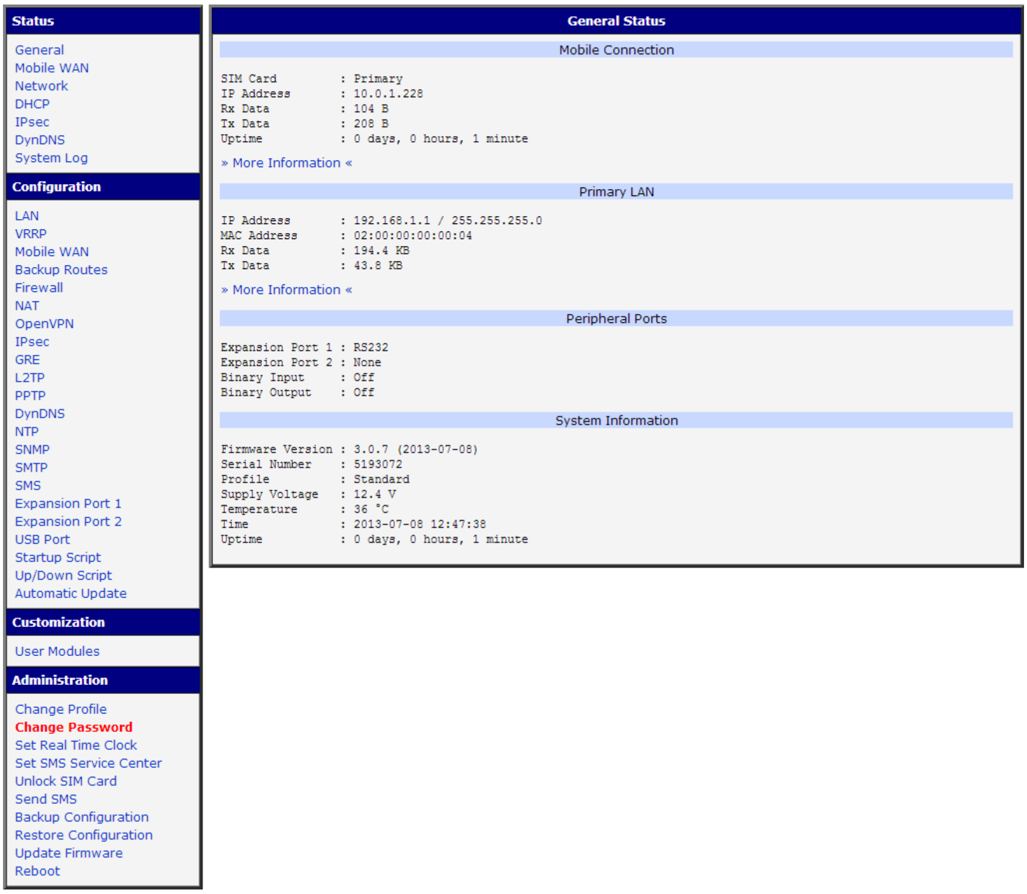
Attention! If the SIM card is not inserted in the router, then wireless transmissions will not work. The inserted SIM card must have activated GPRS. Insert the SIM card when the router is switched-off.

For monitoring, configuring and managing the router use web interface, which can be invoked by entering the IP address of the router into your browser. The default IP address of the router is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

The left part of the web interface contains the menu with pages for monitoring (*Status*), *Configuration*, *Customization* and *Administration* of the router.

Name and *Location* items displays the name and location of the router filled in the SNMP configuration (see SNMP Configuration).

For increased safety of the network managed by the router must be changed the default router password. If the router's default password is set, the *Change password* item is highlighted in red.



```
SIM Card          : Primary
IP Address        : 10.0.1.228
Rx Data           : 104 B
Tx Data           : 208 B
Uptime            : 0 days, 0 hours, 1 minute

IP Address        : 192.168.1.1 / 255.255.255.0
MAC Address       : 02:00:00:00:00:04
Rx Data           : 194.4 KB
Tx Data           : 43.8 KB

Expansion Port 1 : RS232
Expansion Port 2 : None
Binary Input     : Off
Binary Output    : Off

Firmware Version : 3.0.7 (2013-07-08)
Serial Number    : 5193072
Profile          : Standard
Supply Voltage   : 12.4 V
Temperature      : 36 °C
Time             : 2013-07-08 12:47:38
Uptime           : 0 days, 0 hours, 1 minute
```

Figure 1: Web configuration

After green LED starts to blink it is possible to restore initial settings of the router by pressing button RST on front panel. If press button RST, configuration is restored to default and it is reboot (green LED will be on).

1.1 Secured access to web configuration

To the web configuration can be accessed via a secure HTTPS protocol. In the event of a default router IP address is a secure router configuration accessed by entering address https://192.168.1.1 in the web browser. The first approach is the need to install a security certificate. If your browser reports a disagreement in the domain, this message can be prevented use the following procedure.

Since the domain name in the certificate is given the MAC address of the router (such separators are used dashes instead of colons), it is necessary to access the router under this domain name. For access to the router via a domain name, it is adding a DNS record in the DNS table, the operating system.

- Editing /etc/hosts (Linux/Unix)
- Editing C:\WINDOWS\system32\drivers\etc\hosts (Windows XP)
- Configuring your own DNS server

In addition to configuring the router with MAC address 00:11:22:33:44:55 is accessed to secure configuration by typing address https://00-11-22-33-44-55 in the web browser. The first approach is the need to install a security certificate.

When using self signing certificate must upload your files and http_cert http_key directory /etc/certs in the router.

1.2 General

A summary of basic information about the router and its activities can be invoked by selecting the *General* item. This page is also displayed when you login to the web interface. Information is divided into a several of separate blocks according to the type of router activity or the properties area – *Mobile Connection*, *Primary LAN*, *Peripherals Ports* and *System Information*. If your router is equipped with WIFI expansion port, there is also *WIFI* section.

1.2.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card (*Primary* or *Secondary*)
Interface	Defines the interface
IP Address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit

Continued on next page

Continued from previous page

Item	Description
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	Time indicating how long the connection to mobile network is established

Table 1: Mobile connection

1.2.2 Primary LAN

Items displayed in this part have the same meaning as items in the previous part. Moreover, there is information about the MAC address of the router (*MAC Address* item).

1.2.3 Peripheral Ports

Item	Description
Expansion Port 1	Expansion port fitted to the position 1 (*None* indicates that this position is equipped with no port)
Expansion Port 2	Expansion port fitted to the position 2 (*None* indicates that this position is equipped with no port)
Binary Input	State of binary input
Binary Output	State of binary output

Table 2: Peripheral Ports

1.2.4 System Information

Item	Description
Firmware Version	Information about the firmware version

Continued on next page

Continued from previous page

Item	Description
Serial Number	Serial number of the router (in case of *N/A* is not available)
Profile	Current profile – standard or alternative profiles (profiles are used for example to switch between different modes of operation)
Supply Voltage	Supply voltage of the router
Temperature	Temperature in the router
Time	Current date and time
Uptime	Time indicating how long the router is used

Table 3: System Information

1.3 Mobile WAN status

! This item is not available for industrial router XR5i v2.

The *Mobile WAN* menu item contains current information about connections to the mobile network. The first part of this page (*Mobile Network Information*) displays basic information about mobile network in which the router is operated. There is also information about the module, which is mounted in the router.

Item	Description
Registration	State of the network registration
Operator	Specifies the operator in whose network the router is operated
Technology	Transmission technology
PLMN	Code of operator
Cell	Cell to which the router is connected
LAC	Location Area Code – unique number assigned to each location area
Channel	Channel on which the router communicates
Signal Strength	Signal strength of the selected cell
Neighbours	Signal quality of neighboring hearing cells
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI number of module

Table 4: Mobile Network Information

i Highlighted in red adjacent cells have a close signal quality, which means that there is imminence of frequent switching between the current and the highlighted cell.

The next section of this window displays information about the quality of the connection in each period.

Period	Description
Today	Today from 0:00 to 23:59
Yesterday	Yesterday from 0:00 to 23:59
This week	This week from Monday 0:00 to Sunday 23:59
Last week	Last week from Monday 0:00 to Sunday 23:59
This period	This accounting period
Last period	Last accounting period

Table 5: Description of period

Item	Description
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of the router via the mobile network (expressed as a percentage)

Table 6: Mobile Network Statistics

Tips for *Mobile Network Statistics* table:

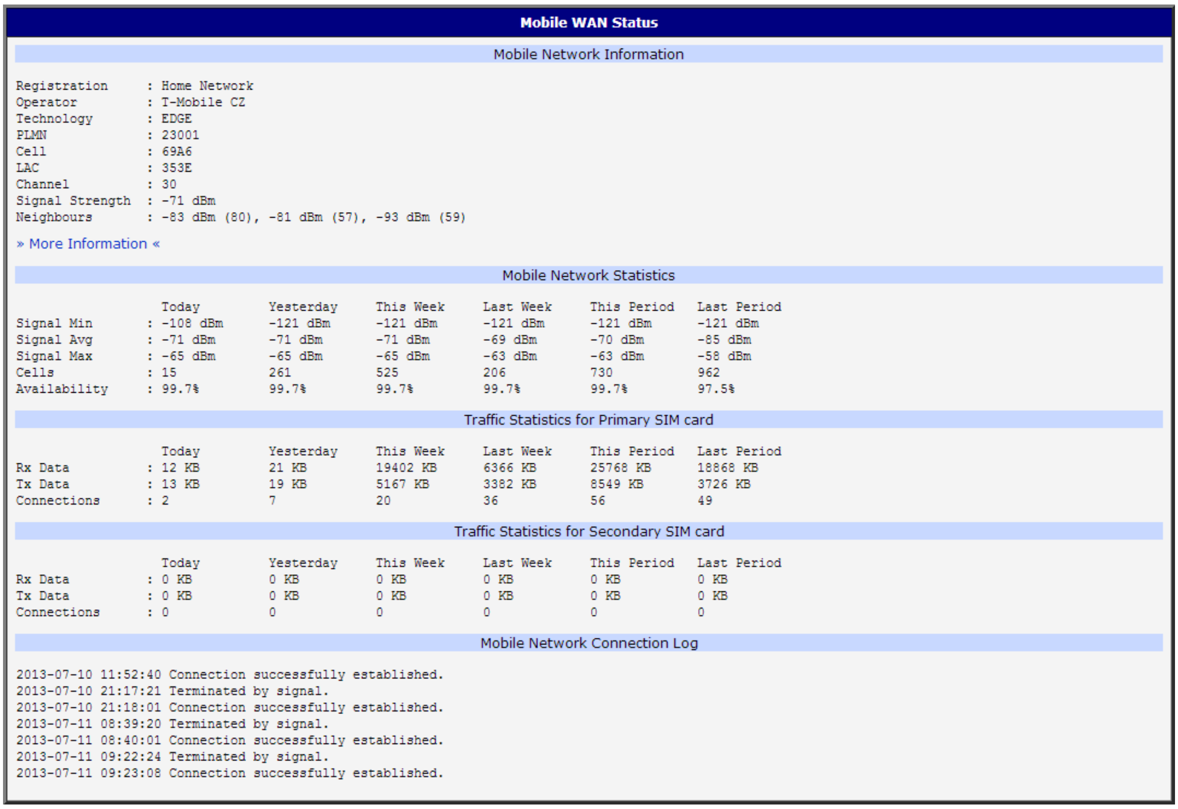
- Availability of connection to mobile network is information expressed as a percentage that is calculated by the ratio of time when connection to mobile network is established to the time when the router is turned on.
- After you place your cursor on the maximum or minimum signal strength, the last time when the router reached this signal strength is displayed.

In the middle part of this page is displayed information about transferred data and number of connections for both SIM card (for each period).

Item	Description
RX data	Total volume of received data
TX data	Total volume of sent data
Connections	Number of connection to mobile network establishment

Table 7: Traffic statistics

The last part (*Mobile Network Connection Log*) informs about the mobile network connection and problems in establishment.



Mobile WAN Status

Mobile Network Information

```
Registration      : Home Network
Operator          : T-Mobile CZ
Technology        : EDGE
PLMN              : 23001
Cell              : 69A6
LAC               : 353E
Channel           : 30
Signal Strength   : -71 dBm
Neighbours        : -83 dBm (80), -81 dBm (57), -93 dBm (59)
```

» More Information «

Mobile Network Statistics

```
                    Today         Yesterday     This Week     Last Week     This Period   Last Period
Signal Min        : -108 dBm      -121 dBm      -121 dBm      -121 dBm      -121 dBm      -121 dBm
Signal Avg        : -71 dBm       -71 dBm       -71 dBm       -69 dBm       -70 dBm       -85 dBm
Signal Max        : -65 dBm       -65 dBm       -65 dBm       -63 dBm       -63 dBm       -58 dBm
Cells             : 15            261           525           206           730           962
Availability      : 99.7%         99.7%         99.7%         99.7%         99.7%         97.5%
```

Traffic Statistics for Primary SIM card

```
                    Today         Yesterday     This Week     Last Week     This Period   Last Period
Rx Data           : 12 KB         21 KB         19402 KB      6366 KB       25768 KB      18868 KB
Tx Data           : 13 KB         19 KB         5167 KB       3382 KB       8549 KB       3726 KB
Connections       : 2             7             20            36            56            49
```

Traffic Statistics for Secondary SIM card

```
                    Today         Yesterday     This Week     Last Week     This Period   Last Period
Rx Data           : 0 KB          0 KB          0 KB          0 KB          0 KB          0 KB
Tx Data           : 0 KB          0 KB          0 KB          0 KB          0 KB          0 KB
Connections       : 0             0             0             0             0             0
```

Mobile Network Connection Log

```
2013-07-10 11:52:40 Connection successfully established.
2013-07-10 21:17:21 Terminated by signal.
2013-07-10 21:18:01 Connection successfully established.
2013-07-11 08:39:20 Terminated by signal.
2013-07-11 08:40:01 Connection successfully established.
2013-07-11 09:22:24 Terminated by signal.
2013-07-11 09:23:08 Connection successfully established.
```

Figure 2: Mobile WAN status

1.4 Network status

To view system information about the router operation, select the *Network* item in the main menu. The upper part of the window displays detailed information about active interfaces:

Interface	Description
eth0	Networks interface
ppp0	Interface (active connection to GPRS/EDGE)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface

Table 8: Description of interface in network status

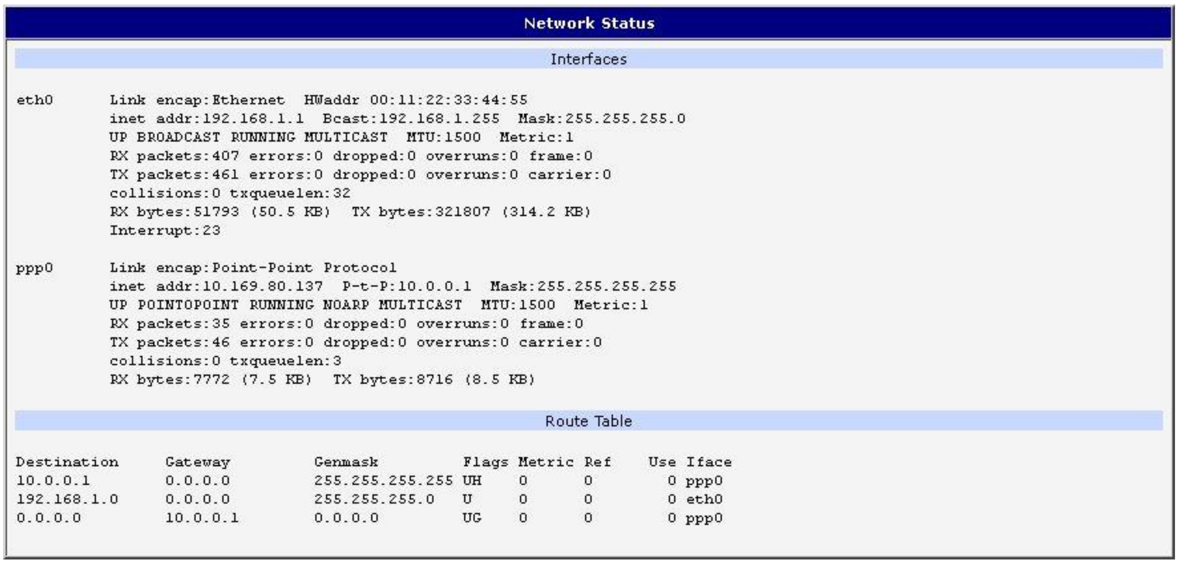
By each of the interfaces is then shown the following information:

Item	Description
HWaddr	Hardware (unique) address of networks interface
inet	IP address of interface
P-t-P	IP address second ends connection
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit
Metric	Number of routers, over which packet must go trought
RX	• packets – received packets • errors – number of errors • dropped – dropped packets • overruns – incoming packets lost because of overload • frame – wrong incoming packets because of incorrect packet size
TX	• packets – transmit packets • errors – number of errors • dropped – dropped packets • overruns – outgoing packets lost because of overload • carrier – wrong outgoing packets with errors resulting from the physical layer
collisions	Number of collisions on physical layer
txqueuelen	Length of front network device
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

Table 9: Description of information in network status

It is possible to read status of connection to mobile network from the network information. If the connection to mobile network is active, then it is in the system information shown as a ppp0 interface.

For industrial router XR5i v2, interface ppp0 indicates PPPoE connection.



Network Status

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 00:11:22:33:44:55
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:407 errors:0 dropped:0 overruns:0 frame:0
          TX packets:461 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:32
          RX bytes:51793 (50.5 KB)  TX bytes:321807 (314.2 KB)
          Interrupt:23

ppp0      Link encap:Point-Point Protocol
          inet addr:10.169.80.137  P-t-P:10.0.0.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:35 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:7772 (7.5 KB)  TX bytes:8716 (8.5 KB)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.1        0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 ppp0
```

Figure 3: Network status

1.5 DHCP status

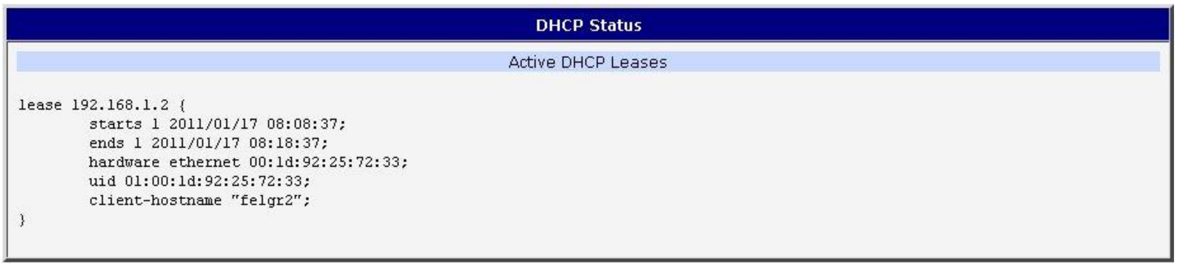
Information on the activities of the DHCP server can be accessed by selecting the *DHCP status* item.

DHCP status informs about activities DHCP server. The DHCP server provides automatic configuration of devices connected to the network managed router. DHCP server assigns to each device's IP address, netmask, default gateway (IP address of router) and DNS server (IP address of router).

For each configuration, the DHCP status window displays the following information.

Item	Description
lease	Assigned IP address
starts	Time of assignation of IP address
ends	Time of termination IP address validity
hardware ethernet	Hardware MAC (unique) address
uid	Unique ID
client-hostname	Computer name

Table 10: DHCP status description



DHCP Status

Active DHCP Leases

```
lease 192.168.1.2 {
        starts 1 2011/01/17 08:08:37;
        ends 1 2011/01/17 08:18:37;
        hardware ethernet 00:1d:92:25:72:33;
        uid 01:00:1d:92:25:72:33;
        client-hostname "felgr2";
}
```

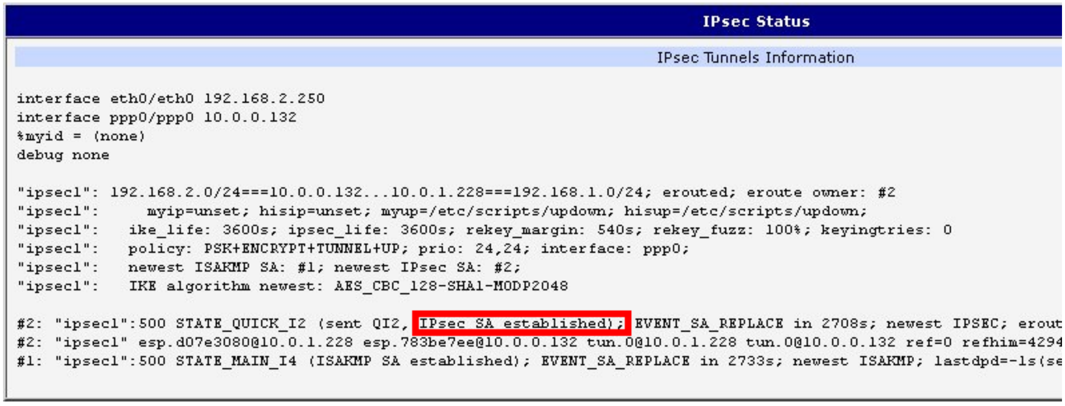
Figure 4: DHCP status

In the extreme, the DHCP status can display two records for one IP address. That could have been caused by resetting of network cards.

1.6 IPsec status

Information on actual IPsec tunnel state can be called up in option *IPsec* in the menu.

After correct build the IPsec tunnel, status display *IPsec SA established* (highlighted in red) in IPsec status information. Other information is only internal character.



IPsec Status

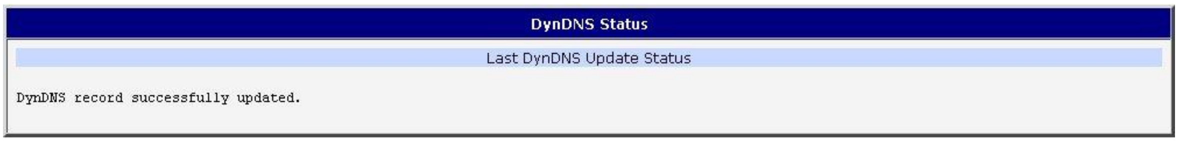
IPsec Tunnels Information

```
interface eth0/eth0 192.168.2.250
interface ppp0/ppp0 10.0.0.132
%myid = (none)
debug none

"ipsec1": 192.168.2.0/24===10.0.0.132...10.0.1.228===192.168.1.0/24; erouted; eroute owner: #2
"ipsec1":     myip=unset; hisip=unset; myup=/etc/scripts/updown; hisup=/etc/scripts/updown;
"ipsec1":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsec1":   policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;
"ipsec1":   newest ISAKMP SA: #1; newest IPsec SA: #2;
"ipsec1":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048

#2: "ipsec1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2708s; newest IPSEC; erout
#2: "ipsec1" esp.d07e3080@10.0.1.228 esp.783be7ee@10.0.0.132 tun.0@10.0.1.228 tun.0@10.0.0.132 ref=0 refhim=4294
#1: "ipsec1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2733s; newest ISAKMP; lastdpd=-1s(se
```

Figure 5: IPsec status

1.7 DynDNS status

DynDNS up – dating entry result on server www.dyndns.org can be called up in option *DynDNS* item in the menu.



DynDNS Status

Last DynDNS Update Status

```
DynDNS record successfully updated.
```

Figure 6: DynDNS status

In detecting the status of updates DynDNS record are possible following message:

- DynDNS client is disabled.
- Invalid username or password.
- Specified hostname doesn't exist.
- Invalid hostname format.
- Hostname exists, but not under specified username.
- No update performed yet.
- DynDNS record is already up to date.
- DynDNS record successfully update.
- DNS error encountered.
- DynDNS server failure.

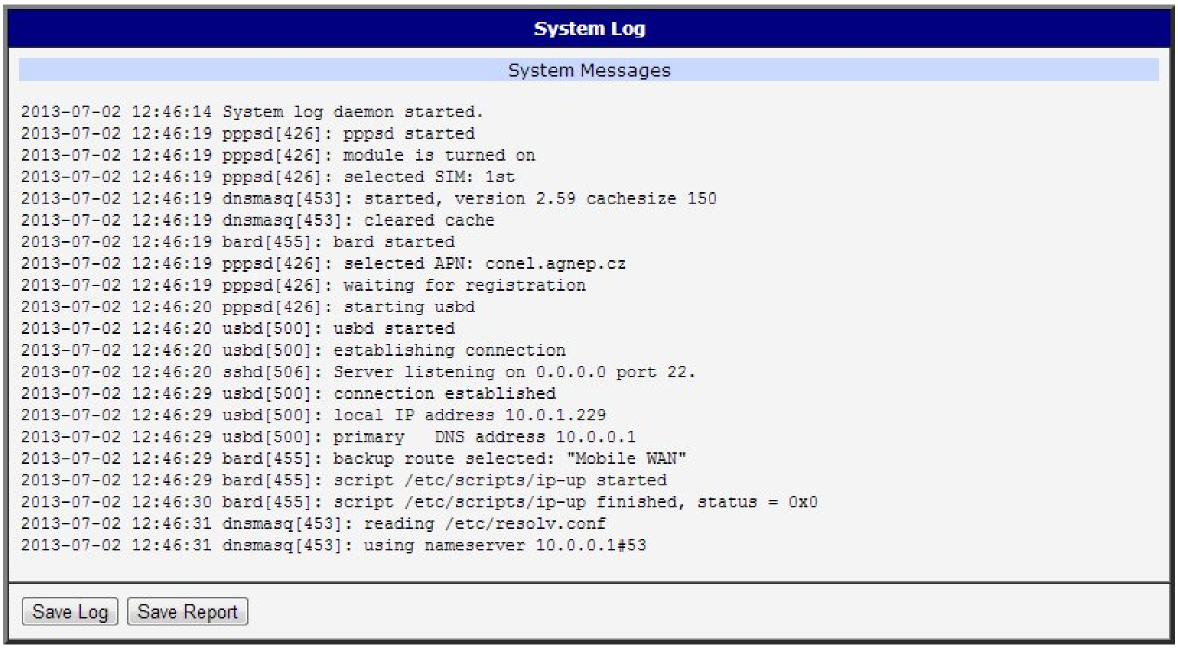
! For correct function DynDNS, SIM card of router must have assigned public IP address.

1.8 System Log

In case of any problems with connection to GPRS it is possible to view the system log by pressing the *System Log* menu item. In the window, are displayed detailed reports from individual applications running in the router. Use the *Save Log* button to save the system log to a connected computer. The second button – *Save Report* – is used for creating detailed report (generates all support needed information in one file).

The Syslog default size is 1000 lines. After reaching 1000 lines create a new file for storing system log. After completion of the 1000 lines in the second file, the first file is deleted and creates a new one.

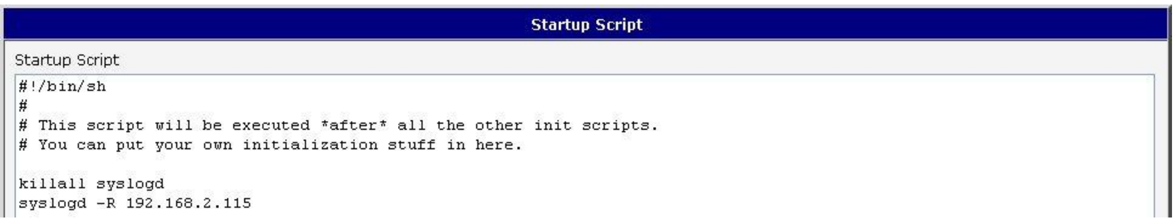
Program syslogd can be started with two options that modifies its behavior. Option "-s" followed by decimal number set maximal number of lines in one log file. Option "-r" followed by hostname or IP address enable logging to remote syslog daemon. In the Linux must be enabled remote logging on the target computer. Typically running syslogd with the parameter “-r”. On Windows must be installed the syslog server (for example Syslog Watcher). For starting syslogd with these options you could modify script "/etc/init.d/syslog" or add lines "killall syslogd" and "syslogd <options> &" into Startup Script.



```
2013-07-02 12:46:14 System log daemon started.
2013-07-02 12:46:19 pppsd[426]: pppsd started
2013-07-02 12:46:19 pppsd[426]: module is turned on
2013-07-02 12:46:19 pppsd[426]: selected SIM: 1st
2013-07-02 12:46:19 dnsmasq[453]: started, version 2.59 cachesize 150
2013-07-02 12:46:19 dnsmasq[453]: cleared cache
2013-07-02 12:46:19 bard[455]: bard started
2013-07-02 12:46:19 pppsd[426]: selected APN: conel.agnep.cz
2013-07-02 12:46:19 pppsd[426]: waiting for registration
2013-07-02 12:46:20 pppsd[426]: starting usbd
2013-07-02 12:46:20 usbd[500]: usbd started
2013-07-02 12:46:20 usbd[500]: establishing connection
2013-07-02 12:46:20 sshd[506]: Server listening on 0.0.0.0 port 22.
2013-07-02 12:46:29 usbd[500]: connection established
2013-07-02 12:46:29 usbd[500]: local IP address 10.0.1.229
2013-07-02 12:46:29 usbd[500]: primary   DNS address 10.0.0.1
2013-07-02 12:46:29 bard[455]: backup route selected: "Mobile WAN"
2013-07-02 12:46:29 bard[455]: script /etc/scripts/ip-up started
2013-07-02 12:46:30 bard[455]: script /etc/scripts/ip-up finished, status = 0x0
2013-07-02 12:46:31 dnsmasq[453]: reading /etc/resolv.conf
2013-07-02 12:46:31 dnsmasq[453]: using nameserver 10.0.0.1#53
```

Figure 7: System Log

Example of logging into the remote daemon at 192.168.2.115:



```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

killall syslogd
syslogd -R 192.168.2.115
```

Figure 8: Example program syslogd start with the parameter -r

1.9 LAN configuration

To enter the network configuration, select the *LAN* menu item. ETH network set in *Primary LAN* configuration, expansion PORT ETH set in *Secondary* LAN configuration.

Item	Description
DHCP Client	• disabled – The router does not allow automatic allocation IP address from a DHCP server in LAN network. • enabled – The router allows automatic allocation IP address from a DHCP server in LAN network.
IP address	Fixed set IP address of network interface ETH.
Subnet Mask	IP address of Subnet Mask.
Bridged	• no – The router is not used as a bridge (default) • yes – The router is used as a bridge
Media type	• Auto-negation – The router selects the speed of communication of network options. • 100 Mbps Full Duplex – The router communicates at 100Mbps, in the full duplex mode. • 100 Mbps Half Duplex – The router communicates at 100Mbps, in the half duplex mode. • 10 Mbps Full Duplex – The router communicates at 10Mbps, in the full duplex mode. • 10 Mbps Half Duplex – The router communicates at 10Mbps, in the half duplex mode.
Default Gateway	IP address of router default gateway. When entering IP address of default gateway, all packets for which the record was not found in the routing table, sent to this address.
DNS server	IP address of DNS server of router. Address where they are forwarded to all DNS questions on the router.

Table 11: Configuration of network interface

There can be only one active bridge on the router at the moment. Only parameters DHCP Client, IP address and Subnet Mask can be used to configure bridge. Primary LAN has got higher priority in this respect when both interfaces (eth0, eth1) are added to the bridge. Other interfaces (wlan0 – wifi) can be added (or deleted) to (from) existing bridge at any moment. Moreover, the bridge can be created on demand of such interfaces but not configured by their respective parameters.

DHCP server assigns IP address, gateway IP address (IP address of the router) and IP address of the DNS server (IP address of the router) to the connected clients.

DHCP server supports static and dynamic assignment of IP addresses. Dynamic DHCP server assigns clients IP addresses from a defined address space. Static DHCP assigns IP addresses that correspond to the MAC addresses of connected clients.

Item	Description
Enable dynamic DHCP leases	If this option is checked, dynamic DHCP server is enable.
IP Pool Start	Start IP addresses space to be allocated to the DHCP clients.
IP Pool End	End IP addresses space to be allocated to the DHCP clients.
Lease time	Time in seconds, after which the client can use IP address.

Table 12: Configuration of dynamic DHCP server

Item	Description
Enable static DHCP leases	If this option is checked, static DHCP server is enable.
MAC Address	MAC address of a DHCP client.
IP Address	Assigned IP address.

Table 13: Configuration of static DHCP server

It is important not to overlap ranges of static allocated IP address with address allocated by the dynamic DHCP. Then risk collision of IP addresses and incorrect function of network.

Example of the network interface with dynamic DHCP server:

- The range of dynamic allocated addresses from 192.168.1.2 to 192.168.1.4.
- The address is allocated 600 second (10 minutes).

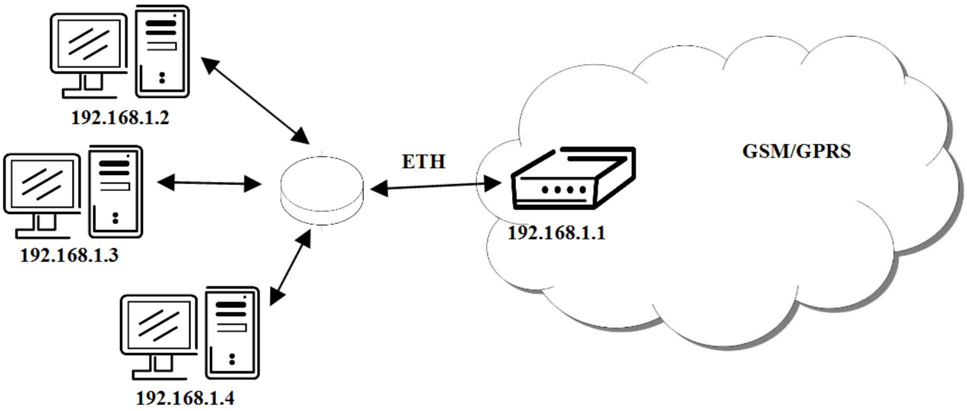
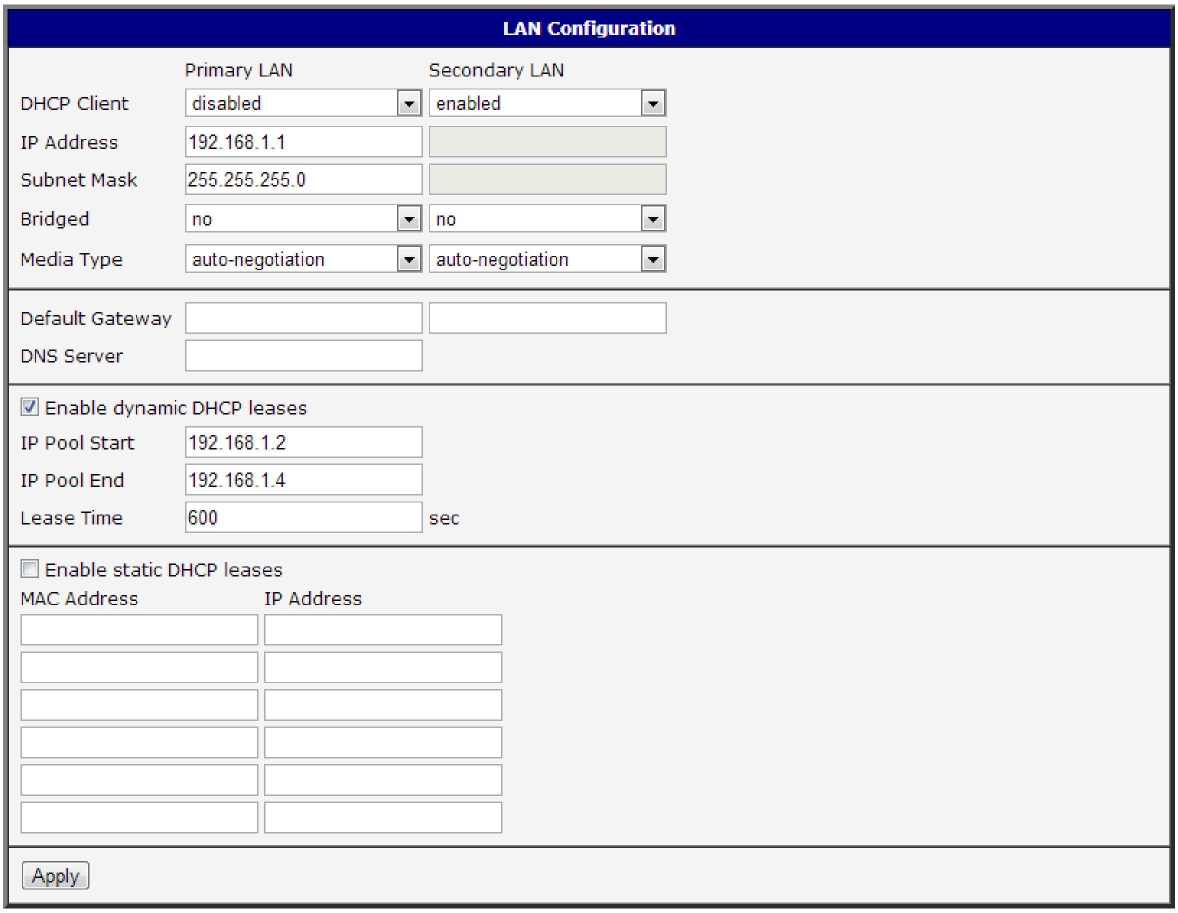


Figure 9: Topology of example LAN configuration 1



LAN Configuration

	Primary LAN	Secondary LAN
DHCP Client	disabled	enabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no	no
Media Type	auto-negotiation	auto-negotiation
Default Gateway		
DNS Server		

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	sec

☐ Enable static DHCP leases

MAC Address	IP Address

Figure 10: Example LAN configuration 1

Example of the network interface with dynamic and static DHCP server:

- The range of allocated addresses from 192.168.1.2 to 192.168.1.4.
- The address is allocated 10 minutes.
- Client's with MAC address 01:23:45:67:89:ab has IP address 192.168.1.10.
- Client's with MAC address 01:54:68:18:ba:7e has IP address 192.168.1.11.

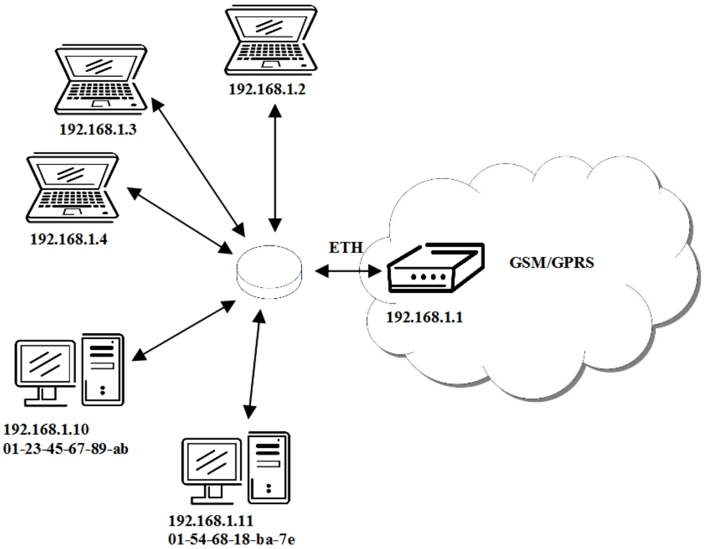
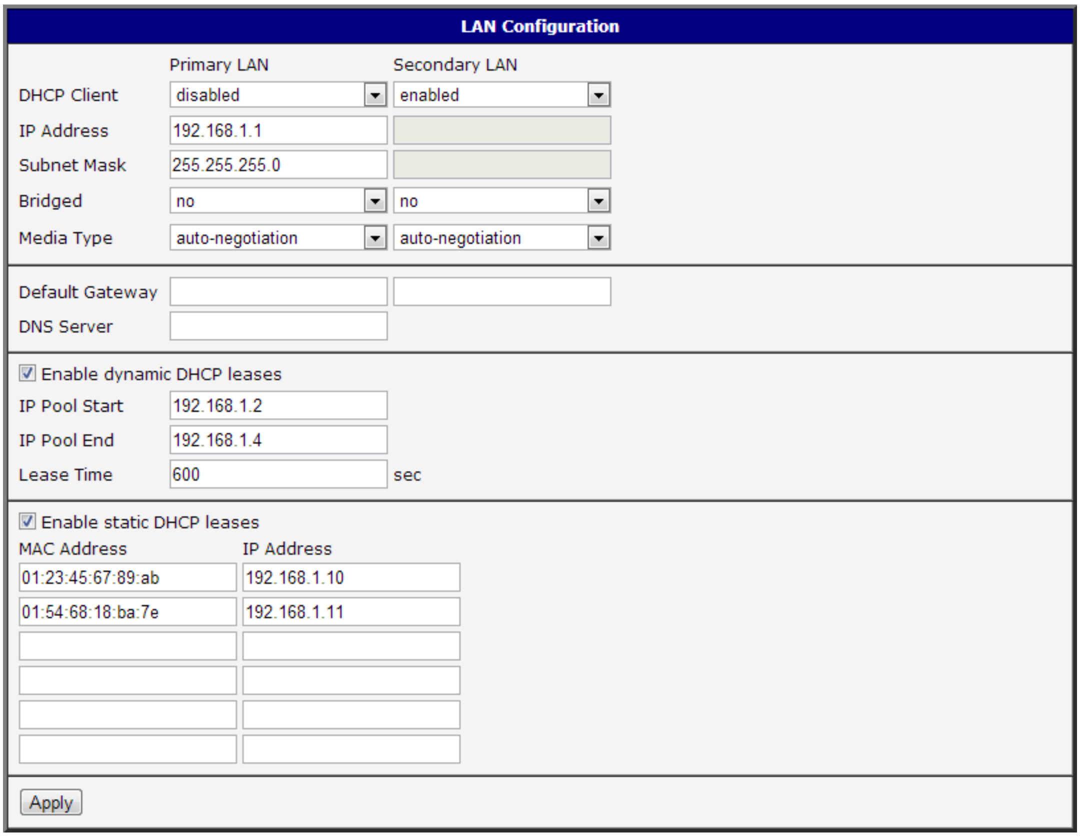


Figure 11: Topology of example LAN configuration 2



LAN Configuration

	Primary LAN	Secondary LAN
DHCP Client	disabled	enabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no	no
Media Type	auto-negotiation	auto-negotiation
Default Gateway		
DNS Server		

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	sec

☑ Enable static DHCP leases

MAC Address	IP Address
01:23:45:67:89:ab	192.168.1.10
01:54:68:18:ba:7e	192.168.1.11

Figure 12: Example LAN configuration 2

Example of the network interface with default gateway and DNS server:

- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20

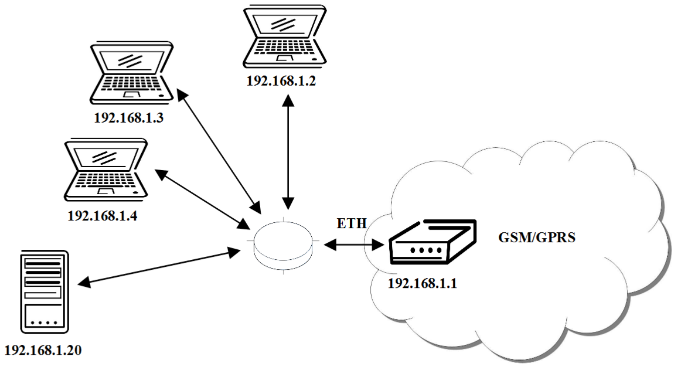
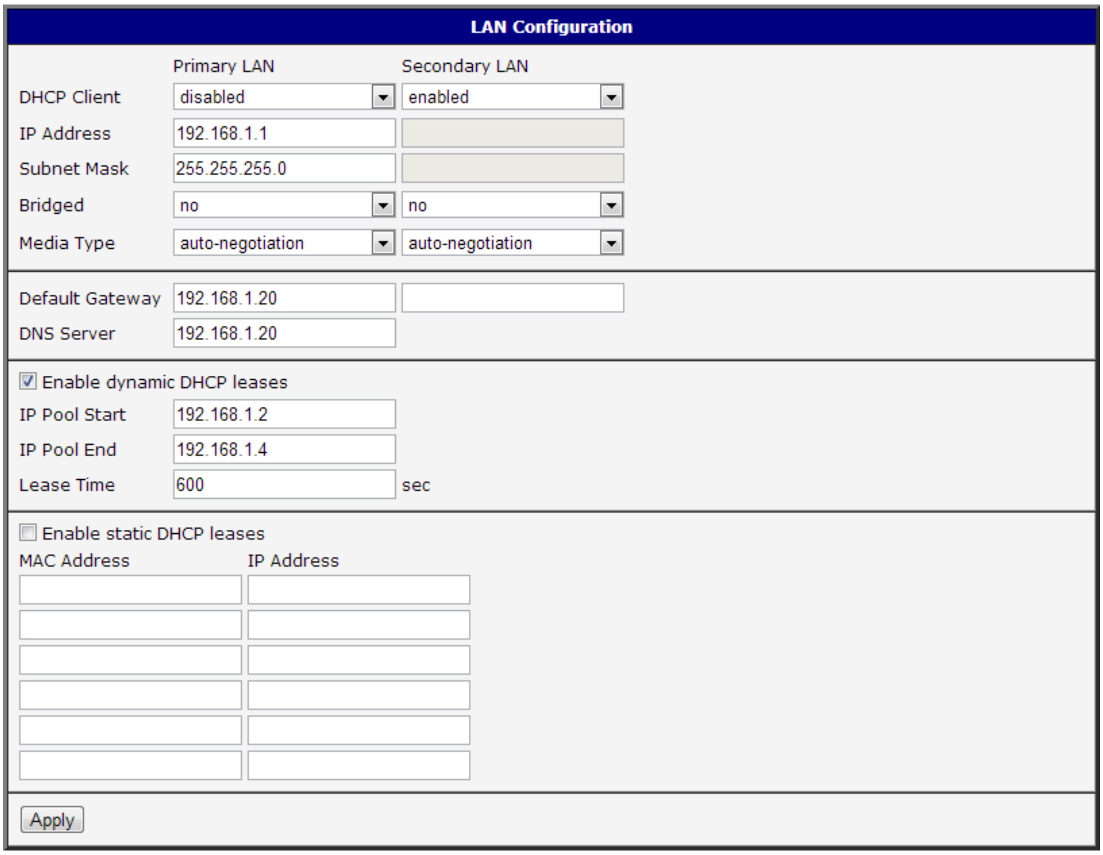


Figure 13: Topology of example LAN configuration 3



LAN Configuration

	Primary LAN	Secondary LAN
DHCP Client	disabled	enabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no	no
Media Type	auto-negotiation	auto-negotiation
Default Gateway	192.168.1.20	
DNS Server	192.168.1.20	

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2	
IP Pool End	192.168.1.4	
Lease Time	600	sec

□ Enable static DHCP leases

MAC Address	IP Address

Figure 14: Example LAN configuration 3

1.10 VRRP configuration

To enter the VRRP configuration select the *VRRP* menu item. VRRP protocol (Virtual Router Redundancy Protocol) is a technique, by which it is possible to forward routing from main router to backup router in the case of the main router failure. If the *Enable VRRP* is checked, then it is possible to set the following parameters.

Item	Description
Virtual Server IP Address	This parameter sets virtual server IP address. This address should be the same for both routers. A connected device sends its data via this virtual address.
Virtual Server ID	Parameter Virtual Server ID distinguishes one virtual router on the network from others. Main and backup routers must use the same value for this parameter.
Host Priority	The router, with higher priority set by the parameter Host Priority, is the main router. According to RFC 2338 the main router has the highest possible priority - 255. The backup router has priority in range 1 – 254 (init value is 100). The priority value equals 0 is not allowed.

Table 14: VRRP configuration

It is possible to set *Check connection* flag in the second part of the window. The currently active router (main/backup) will send testing messages to defined *Ping IP Address* at periodic time intervals (*Ping Interval*) with setting time of waiting for answer (*Ping Timeout*). The function check connection is used as a supplement of VRRP standard with the same final result. If there are no answers from remote devices (*Ping IP Address*) for a defined number of probes (*Ping Probes*), then connection is switched to the other line.

Item	Description
Ping IP Address	Destinations IP address ping queries. Address can not specify as domain name.
Ping Interval	Time intervals between the outgoing pings.
Ping Timeout	Time to wait to answer.
Ping Probes	Number of failed ping requests, after which the route is considered to be impassable.

Table 15: Check connection

Ping IP address is possible to use for example a DNS server of mobile operator as a test message (ping) IP address.

There's an additional way for evaluating the state of the active line. It is activated by selecting *Enable traffic monitoring* parameter. If this parameter is set and any packet different from ping is sent to the monitored line, then any answer to this packet is expected for *Ping Timeout*.

If *Ping Timeout* expires with no answer received then process of testing the active line continues the same way like in the case of standard testing process after first test message answer drops out.

Example of the VRRP protocol:

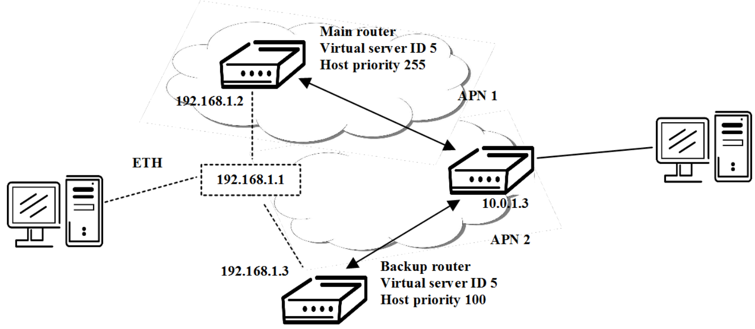
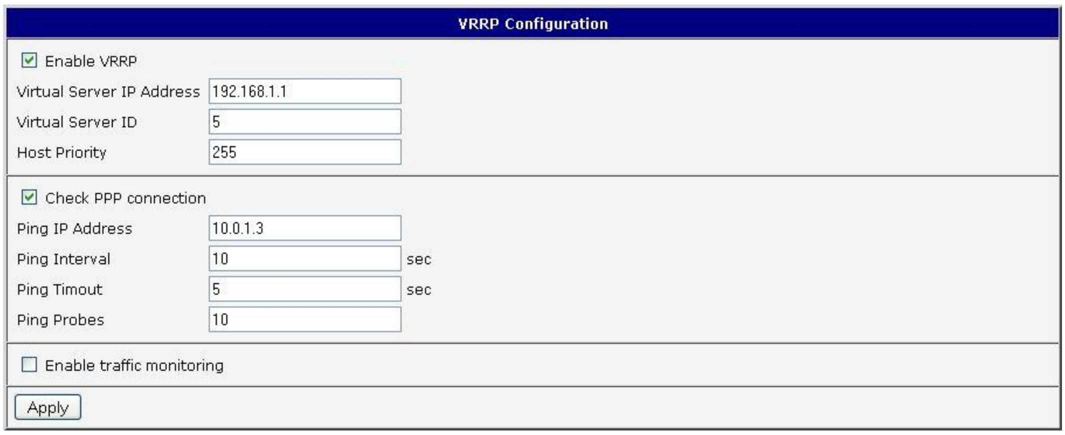


Figure 15: Topology of example VRRP configuration



VRRP Configuration

☑ Enable VRRP

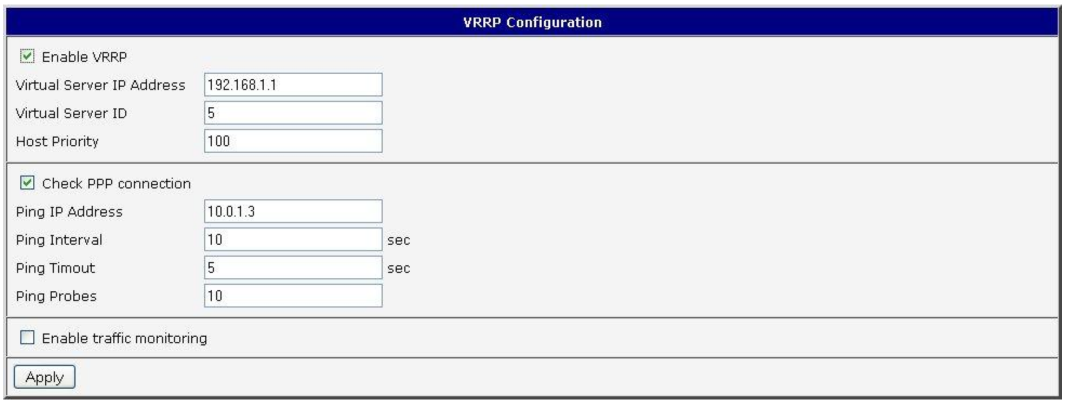
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	255

☑ Check PPP connection

Ping IP Address	10.0.1.3	
Ping Interval	10	sec
Ping Timout	5	sec
Ping Probes	10	

☐ Enable traffic monitoring

Figure 16: Example VRRP configuration — main router



VRRP Configuration

☑ Enable VRRP

Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	100

☑ Check PPP connection

Ping IP Address	10.0.1.3	
Ping Interval	10	sec
Ping Timout	5	sec
Ping Probes	10	

☐ Enable traffic monitoring

Figure 17: Example VRRP configuration -– backup router

1.11 Mobile WAN configuration

! This item is not available for industrial router XR5i v2.

The form for configuration of a connection to the mobile network can be invoked by selecting the *Mobile WAN* item in the main menu of the router web interface.

1.11.1 Connection to mobile network

If the *Create connection to mobile network* item is selected, the router automatically tries to establish connection after switching-on.

Item	Description
Carrier	Defines carrier and used transmission technology
APN	Network identifier (Access Point Name)
Username	User name to log into the GSM network
Password	Password to log into the GSM network
Authentication	Authentication protocol in GSM network: • PAP or CHAP – Router is chosen one of the authentication methods. • PAP – It is used PAP authentication method. • CHAP – It is used CHAP authentication method.
IP Address	IP address of SIM card. The user sets the IP address, only in the case IP address was assigned of the operator.
Phone Number	Telephone number to dial GPRS or CSD connection. Router as a default telephone number used *99***1 #.
Operator	This item can be defined PLNM preferred carrier code
Network type	• Automatic selection – Router automatically selects a specific transmission method according to the availability of transmission technology. • Furthermore, according to the type of router – it is also possible to select a specific method of data transmission (GPRS, UMTS, . . .).
PIN	PIN parameter should be set only if it requires a SIM card router. SIM card is blocked in case of several bad attempts to enter the PIN.
MRU	Maximum Receiving Unit – It's an identifier of maximum size of packet, which is possible to receive in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.
MTU	Maximum Transmission Unit – It's an identifier of max. size of packet, which is possible to transfer in a given environment. Default value is 1500 B. Other settings may cause incorrect transmission of data.

Table 16: Mobile WAN connection configuration

Tips for working with the *Mobile WAN* configuration form:

- If the *IP address* field is not filled in, the operator automatically assigns the IP address when it is establishing the connection. If filled IP address supplied by the operator, router accelerate access to the network.
- If the *APN* field is not filled in, the router automatically selects the APN by the IMSI code of the SIM card. If the PLMN (operator number format) is not in the list of APN, then default APN is "internet". The mobile operator defines APN.

ATTENTION:

- **If only one SIM card is plugged in the router, router switches between the APN. Router with two SIM cards switches between SIM cards.**
- **Correct PIN must be filled. For SIM cards with two APN's there will be the same PIN for both APN's. Otherwise the SIM card can be blocked by false SIM PIN.**

Items marked with an asterisk must be filled in only if this information is required by the operator (carrier).

In case of unsuccessful establishing a connection to mobile network is recommended to check the accuracy of entered data. Alternatively, try a different authentication method or network type.

1.11.2 DNS address configuration

The choice *Get DNS address from operator* is given for easier configuration on client side. If this field is filled in, then the router tries to get an IP address of primary and secondary DNS server from the operator automatically.

1.11.3 Check connection to mobile network configuration

If the *Check connection to mobile network* option is selected, it has active control of connection to mobile network. The router will automatically send the ping question to the selected domain name or IP address in periodic time intervals. If the PING failed, new ping be sent immediately. After three unsuccessfully pings on appropriate IP address the router terminates connection and tries to establish a new connection. It is possible to use, for example, the DNS server of a mobile operator as the ping IP address.

Item	Description
Ping IP Address	Destinations IP address or domain name of ping queries.
Ping Interval	Time intervals between the outgoing pings.

Table 17: Check connection to mobile network configuration

If the *Enable Traffic Monitoring* option is selected, then the router stops sending ping questions to the Ping IP Address and it will watch traffic in connection to mobile network. If this connection is without traffic longer than the Ping Interval, then the router sends ping questions to the Ping IP Address.

Attention! We recommend checking the Check connection to mobile network in case of uninterrupted running.

1.11.4 Data limit configuration

Item	Description
Data limit	With this parameter you can set the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (month).
Warning Threshold	Parameter *Warning Threshold* determine per cent of Data Limit in the range of 50% to 99%, which if is exceeded, then the router sends SMS in the form *Router has exceeded (value of Warning Threshold) of data limit*.
Accounting Start	Parameter sets the day of the month in which the billing cycle starts SIM card used. Start of the billing period defines the operator, which gives the SIM card. The router begin to count the transferred data since that day.

Table 18: Data limit configuration

If parameters *Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded* (see next subsection) or *Send SMS when datalimit is exceeded* (see SMS configuration) are not selected the data limit will not count.

1.11.5 Switch between SIM cards configuration

At the bottom of configuration it is possible to set rules for switching between two APN's on the SIM card, in the event that one SIM card is inserted or between two SIM cards, in the event that two SIM cards are inserted.

Item	Description
Default SIM card	This parameter sets default APN or SIM card, from which it will try to establish the connection to mobile network. If this parameter is set to none, the router launches in offline mode and it is necessary to establish connection to mobile network via SMS message.
Backup SIM card	Defines backup APN or SIM card, that the router will switch the defining one of the following rules.

Table 19: Default and backup SIM configuration

If parameter Backup SIM card is set to none, then parameters *Switch to other SIM card when connection fails*, *Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected* and *Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded* switch the router to off-line mode.

Item	Description
Switch to other SIM card when connection fails	If connection to mobile network fails, then this parameter ensures switch to secondary SIM card or secondary APN of the SIM card. Failure of the connection to mobile network can occur in two ways. When I start the router, when three fails to establish a connection to mobile network. Or if it is checked Check the connection to mobile network, and is indicated by the loss of a connection to mobile network.
Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected	In case that the roaming is detected this parameter enables switching to secondary SIM card or secondary APN of the SIM. If home network is detected, this parameter enables switching back to default SIM card.
Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded	This parameter enables switching to secondary SIM card or secondary APN of the SIM card, when the data limit of default APN is exceeded. This parameter also enables switching back to default SIM card, when data limit is not exceeded.
Switch to backup SIM card when binary input is active switch to default SIM card when binary input isn't active	This parameter enables switching to secondary SIM card or secondary APN of the SIM card, when binary input 'bin0' is active. If binary input isn't active, this parameter enables switching back to default SIM card.
Switch to default SIM card after timeout	This parameter defines the method, how the router will try to switch back to default SIM card or default APN.

Table 20: Switch between SIM card configurations

The following parameters define the time after which the router attempts to go back to the default SIM card or APN.

Item	Description
Initial timeout	The first attempt to switch back to the primary SIM card or APN shall be made for the time defined in the parameter Initial Timeout, range of this parameter is from 1 to 10000 minutes.

Continued on next page

Continued from previous page

Item	Description
Subsequent Timeout	In an unsuccessful attempt to switch to default SIM card, the router on the second attempt to try for the time defined in the parameter Subsequent Timeout, range is from 1 to 10000 min.
Additive constants	Any further attempt to switch back to the primary SIM card or APN shall be made in time computed as the sum of the previous time trial and time defined in the parameter Additive constants range is 1-10000 minutes.

Table 21: Switch between SIM card configurations

Example:
If parameter *Switch to default SIM card after timeout* is checked and parameters are set as follows: *Initial Timeout* – 60 min, *Subsequent Timeout* 30 min and *Additive Timeout* – 20 min, the first attempt to switch the primary SIM card or APN shall be carried out after 60 minutes. Switched to a failed second attempt made after 30 minutes. Third after 50 minutes (30+20). Fourth after 70 minutes (30+20+20).

1.11.6 Dial-In access configuration

Dial-In access configuration is supported only for these routers: ER75i, UR5, ER75i v2 and UR5 v2.

In the bottom part of the window it is possible to define access over CSD connection by *Enable Dial-In Access* function. Access can be secured by used the *Username* and *Password*. In the event that this function is enabled and the router does not have a connection to mobile network is granted access to the router via dial-up connections CSD. The router waits 2 minutes to accept connections. If the router during this time nobody logs on, the router will try again to establish a GPRS connection.

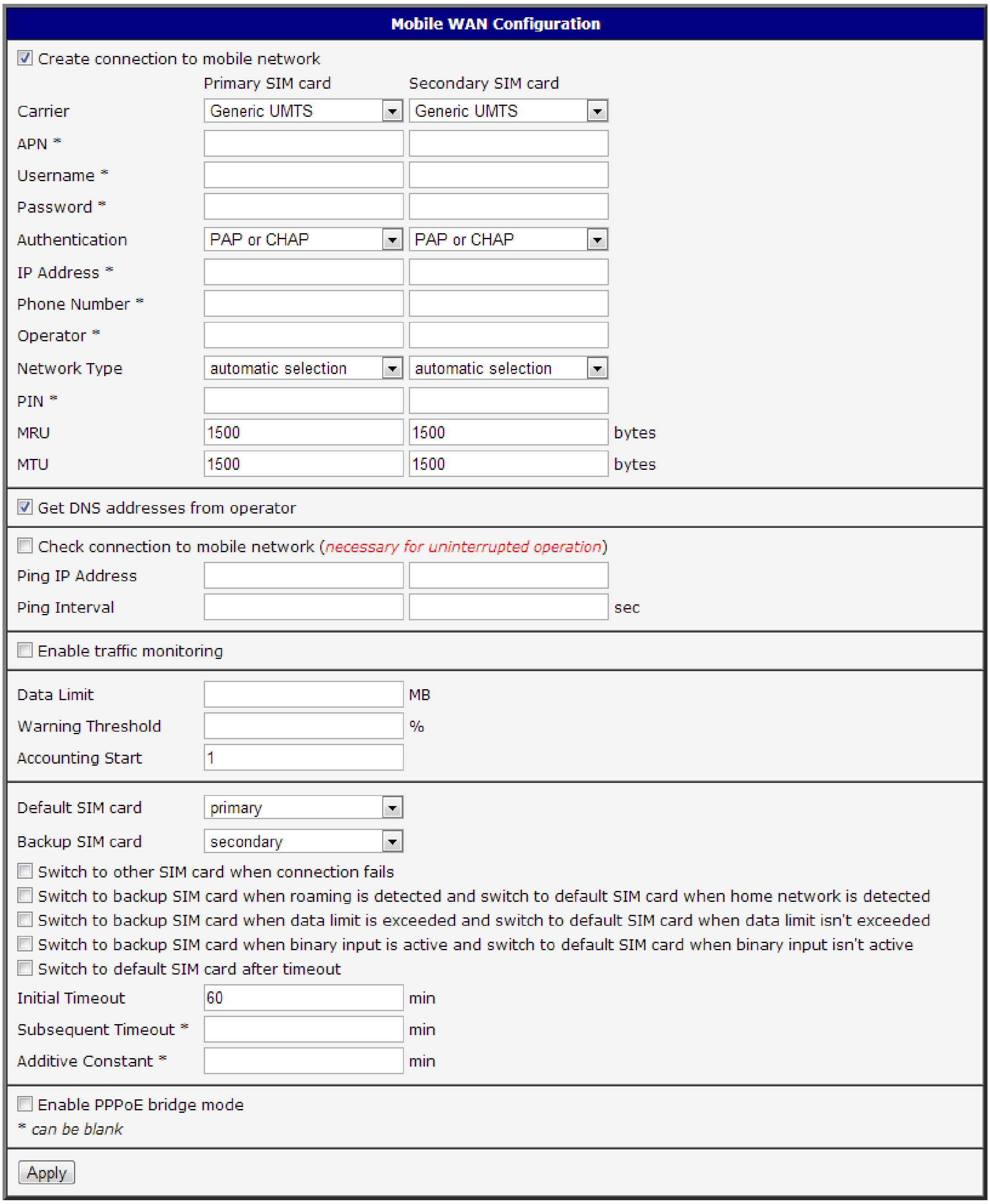
Item	Description
Username	User name for secured Dial-In access.
Password	Password for secured Dial-In access.

Table 22: Dial-In access configuration

1.11.7 PPPoE bridge mode configuration

If the *Enable PPPoE bridge mode* option selected, it activate the PPPoE bridge protocol PPPoE (point-to-point over ethernet) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. Allows you to create a PPPoE connection from the device behind router. For example from PC which is connected to ETH port router. There will be allot Ip address of SIM card to PC.

The changes in settings will apply after pressing the *Apply* button.



Mobile WAN Configuration

☑ Create connection to mobile network

	Primary SIM card	Secondary SIM card	
Carrier	Generic UMTS	Generic UMTS	
APN *			
Username *			
Password *			
Authentication	PAP or CHAP	PAP or CHAP	
IP Address *			
Phone Number *			
Operator *			
Network Type	automatic selection	automatic selection	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes

☑ Get DNS addresses from operator

☐ Check connection to mobile network (*necessary for uninterrupted operation*)

Ping IP Address			
Ping Interval			sec

☐ Enable traffic monitoring

Data Limit		MB
Warning Threshold		%
Accounting Start	1	

Default SIM card	primary
Backup SIM card	secondary

☐ Switch to other SIM card when connection fails

☐ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected

☐ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded

☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active

☐ Switch to default SIM card after timeout

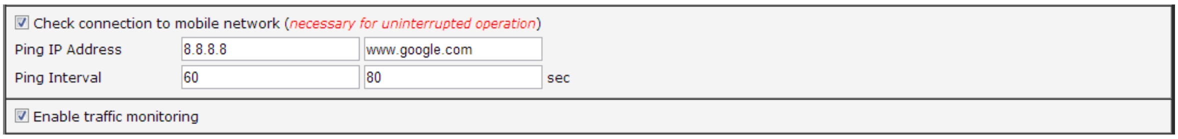
Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

☐ Enable PPPoE bridge mode

** can be blank*

Figure 18: Mobile WAN configuration

The figure below describes the situation, when the connection to mobile network is controlled on the address 8.8.8.8 in the time interval of 60 s for primary SIM card and on the address www.google.com in the time interval 80 s for secondary SIM card. In the case of traffic on the router the control pings are not sent, but the traffic is monitored.



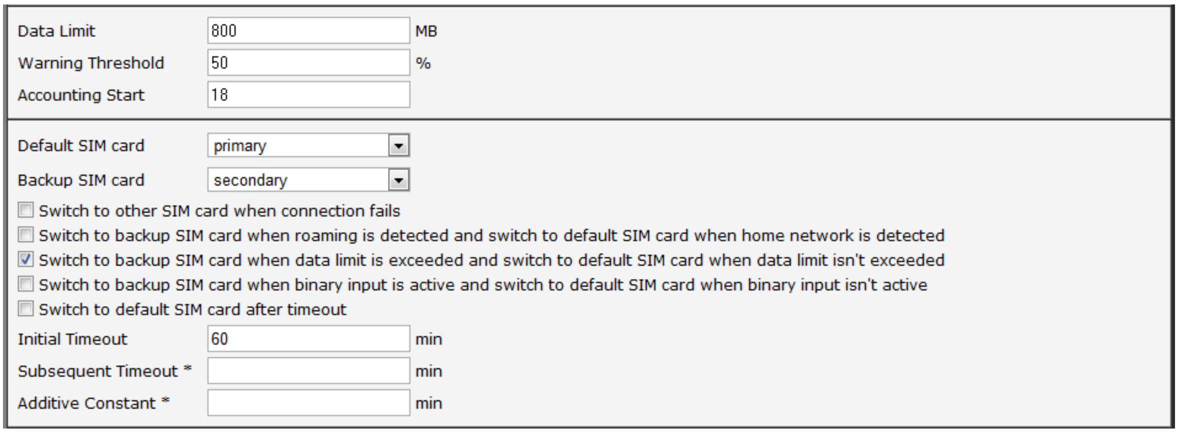
☑ Check connection to mobile network (*necessary for uninterrupted operation*)

Ping IP Address	8.8.8.8	www.google.com	
Ping Interval	60	80	sec

☑ Enable traffic monitoring

Figure 19: Example of Mobile WAN configuration 1

he following configuration illustrates the situation in which the router switches to a backup SIM card after exceeding the data limits of 800 MB. Warning SMS is sent upon reaching 400 MB. The start of accounting period is set to the 18th day of the month.



Data Limit	800	MB
Warning Threshold	50	%
Accounting Start	18	

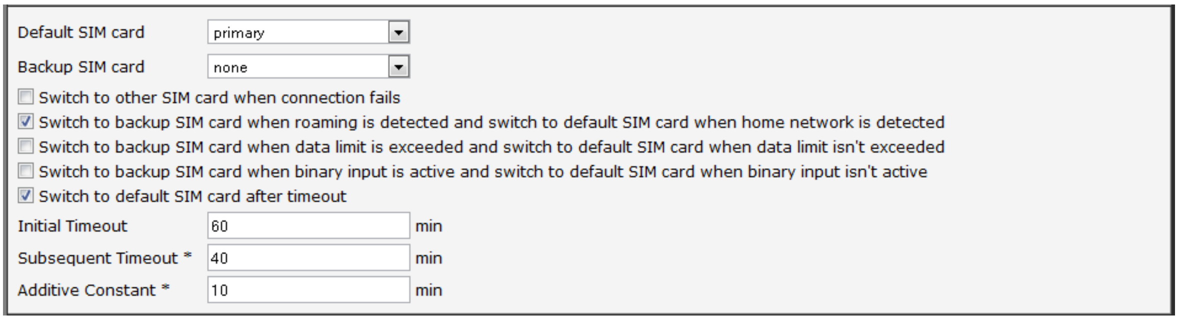
Default SIM card	primary
Backup SIM card	secondary

☐ Switch to other SIM card when connection fails
☐ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
☑ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active
☐ Switch to default SIM card after timeout

Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

Figure 20: Example of Mobile WAN configuration 2

Primary SIM card is switched to the offline mode after the router detects roaming. The first attempt to switch back to the default SIM card is executed after 60 minutes, the second after 40 minutes, the third after 50 minutes (40+10) etc.



Default SIM card	primary
Backup SIM card	none

☐ Switch to other SIM card when connection fails
☑ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
☐ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active
☑ Switch to default SIM card after timeout

Initial Timeout	60	min
Subsequent Timeout *	40	min
Additive Constant *	10	min

Figure 21: Example of Mobile WAN configuration 3

1.12 Backup Routes

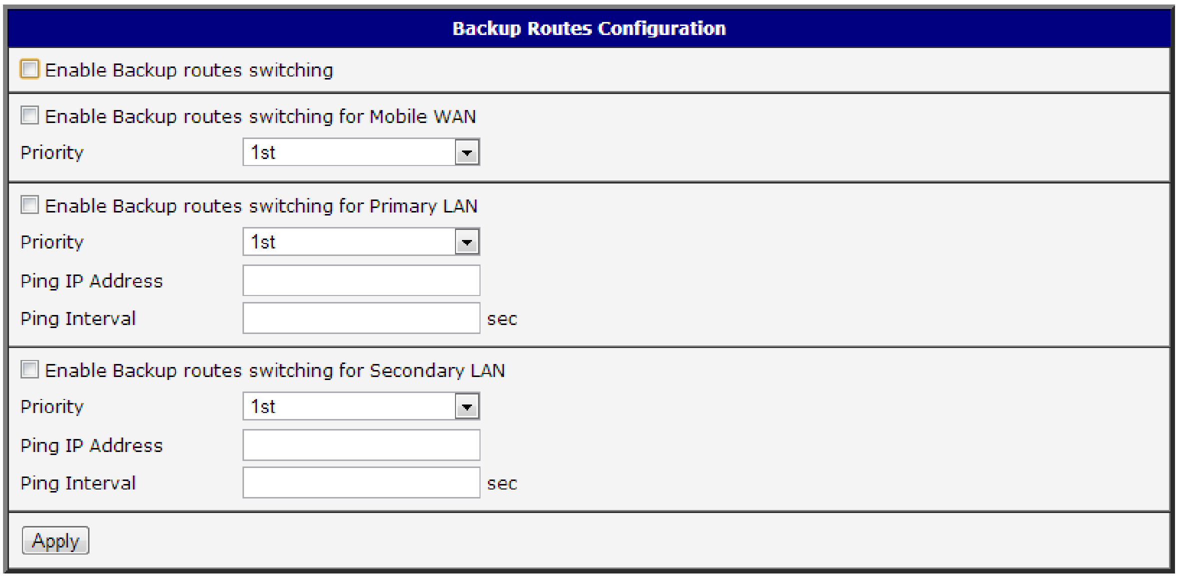
Using the configuration form on the *Backup Routes* page can be set backing up primary connection by other connections to internet/mobile network. For each back up connection can be defined a priority. Own switching is done based on set priorities and state of the connection (for *Primary LAN* and *Secondary LAN*).

It is necessary to check the *Enable backup routes switching* item to enable switching. The check box at the beginning of each section of back up connection allows you to switch to the corresponding type of connection (there are these check boxes: *Enable backup routes switching for Mobile WAN*, *Enable backup routes switching for Primary LAN* and *Enable backup routes switching for Secondary LAN*).

Item	Description
Priority	Priority for the type of connection
Ping IP Address	Destination IP address of ping queries to check the connection **(address can not be specified as a domain name)**
Ping Interval	The time intervals between sent ping queries

Table 23: Backup Routes

All changes in settings will be applied after pressing the *Apply* button.



Backup Routes Configuration

☐ Enable Backup routes switching

☐ Enable Backup routes switching for Mobile WAN

Priority: 1st

☐ Enable Backup routes switching for Primary LAN

Priority: 1st

Ping IP Address:

Ping Interval: sec

☐ Enable Backup routes switching for Secondary LAN

Priority: 1st

Ping IP Address:

Ping Interval: sec

Figure 22: Backup Routes

1.13 PPPoE Configuration

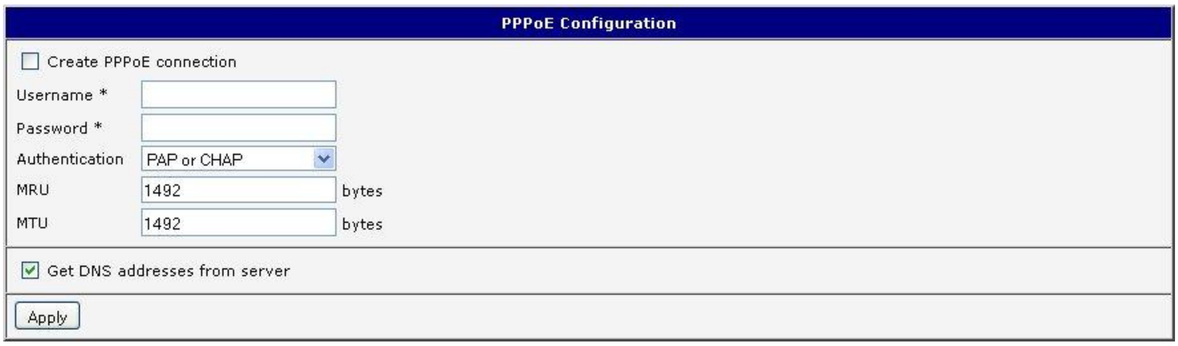
! The *PPPoE Configuration* item is available only for the industrial router XR5i v2.

PPPoE for industrial router works in client mode. Router using connection to the PPPoE server or PPPoE bridge (for example ADSL modem).

To enter the PPPoE configuration select the *PPPoE* menu item. If the *Create PPPoE connection* option is selected, the router tries to establish PPPoE connection after switching-on. PPPoE (Point-to-Point over Ethernet) is a network protocol, which PPP frames encapsulating to the Ethernet frames. PPPoE client to connect devices that support PPPoE bridge or a server (typically ADSL router). After connecting the router obtains the IP address of the device to which it is connected. All communications from the device behind the PPPoE server is forwarded to industrial router.

Item	Description
Username	Username for secure access to PPPoE
Password	Password for secure access to PPPoE
Authentication	Authentication protocol in GSM network ● PAP or CHAP – Router is chosen one of the authentication methods. ● PAP – It is used PAP authentication method. ● CHAP – It is used CHAP authentication method.
MRU	(Maximum Receiving Unit) – it is the identifier of the maximum size of packet, which is possible to recese in given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.
MTU	(Maximum Transmission Unit) – it is the identifier of the maximum size of packet, which is possible to transfer in given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.

Table 24: PPPoE configuration


PPPoE Configuration

☐ Create PPPoE connection

Username *		
Password *		
Authentication	PAP or CHAP	
MRU	1492	bytes
MTU	1492	bytes

☑ Get DNS addresses from server

Figure 23: PPPoE configuration

1.14 Firewall configuration

By the help of a firewall it is possible to set IP addresses from which are possible to remotely access the router and internal network connected behind a router. The choice *Allow remote access only from specified hosts* is given for easier configuration of hosts. In this firewall configuration it is possible to set up to four remote accesses by the help of *Source*, *Source IP Address*, *Protocol* and *Target Port*.

Item	Description
Source	• single address – access allowed a single IP address defined in the Source IP Address, • any address – allowed access to any IP address.
Source IP address	IP address from which it is allowed to access the router.
Source Protocol	Specify protocol for remote access: • all – access is allowed by all, • TCP – access is allowed by TCP, • UDP – access is allowed by UDP, • ICMP – access is allowed by ICMP.
Target Port	The port number on which it is allowed to access the router.

Table 25: Firewall configuration

Example of the firewall configuration:

The router has allowed the following access:

- from address 171.92.5.45 using any protocol
- from address 10.0.2.123 using TCP protocol on any ports
- from address 142.2.26.54 using ICMP protocol

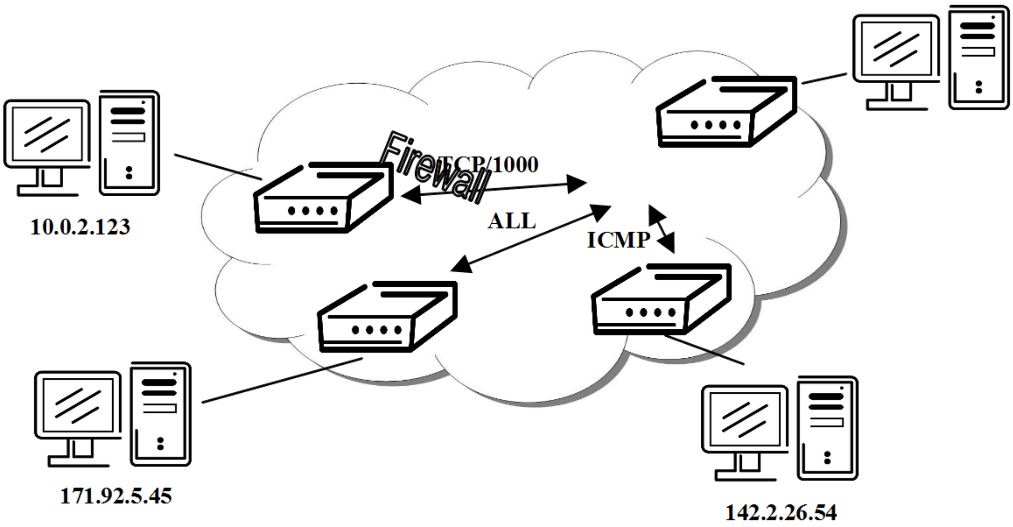
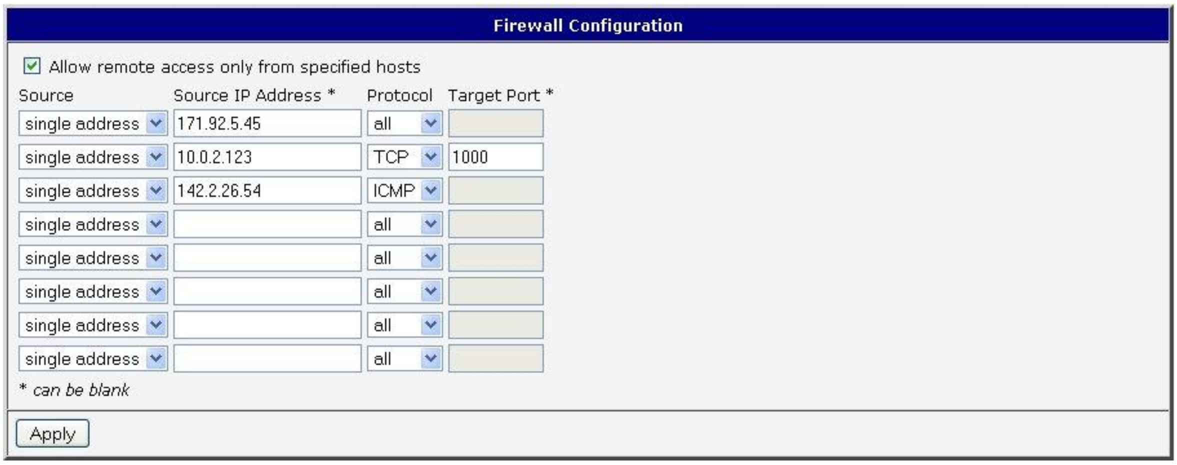


Figure 24: Topology of example firewall configuration



Firewall Configuration

☑ Allow remote access only from specified hosts

Source	Source IP Address *	Protocol	Target Port *
single address	171.92.5.45	all	
single address	10.0.2.123	TCP	1000
single address	142.2.26.54	ICMP	
single address		all	
single address		all	
single address		all	
single address		all	
single address		all	

** can be blank*

Figure 25: Example firewall configuration

1.15 NAT configuration

To enter the Network Address Translation configuration, select the *NAT* menu item. NAT (Network address Translation / Port address Translation - PAT) is a method of adjusting the network traffic through the router default transcript and/or destination IP addresses often change the number of TCP/UDP port for walk-through IP packets. The window contains sixteen entries for the definition of NAT rules.

Item	Description
Public Port	Public port
Private Port	Private port
Type	Protocol selection
Server IP address	IP address which will be forwarded incoming data

Table 26: NAT configuration

If necessary set more than sixteen rules for NAT rules, then is possible insert into start up script following script:

```
iptables -t nat -A napt -p tcp --dport [PORT\_PUBLIC] -j DNAT --to-destination
[IPADDR]:[PORT1\_PRIVATE]
```

Concrete IP address [IPADDR] and ports numbers [PORT_PUBLIC] and [PORT_PRIVATE] are filled up into square bracket.

The following items are used to set the routing of all incoming traffic from the PPP to the connected computer.

Item	Description
Send all remaining incoming packets to default server	By checking this item and setting the Default Server item it is possible to put the router into the mode in which all incoming data from GPRS will be routed to the computer with the defined IP address.
Default Server IP Address	Send all incoming packets to this IP addresses.

Table 27: Configuration of send all incoming packets

Enable the following options and enter the port number is allowed remote access to the router from PPP interface.

Item	Description
Enable remote HTTP access on port	If this item field and port number is filled in, then configuration of the router over web interface is possible (disabled in default configuration).
Enable remote HTTPS access on port	If this item field and port number is filled in, then configuration of the router over web interface is possible (disabled in default configuration).
Enable remote FTP access on port	Choice this item and port number makes it possible to access over FTP (disabled in default configuration).
Enable remote SSH access on port	Choice this item and port number makes it possible to access over SSH (disabled in default configuration).
Enable remote Telnet access on port	Choice this item and port number makes it possible to access over Telnet (disabled in default configuration).
Enable remote SNMP access on port	Choice this item and port number makes it possible to access to SNMP agent.
Masquerade outgoing packets	Choice Masquerade (alternative name for the NAT system) item option turns the system address translation NAT.

Table 28: Remote access configuration

Example of the configuration with one connection equipment on the router:

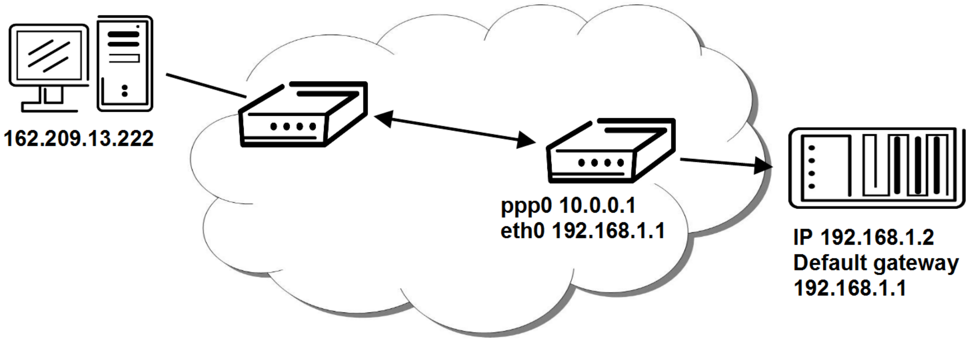
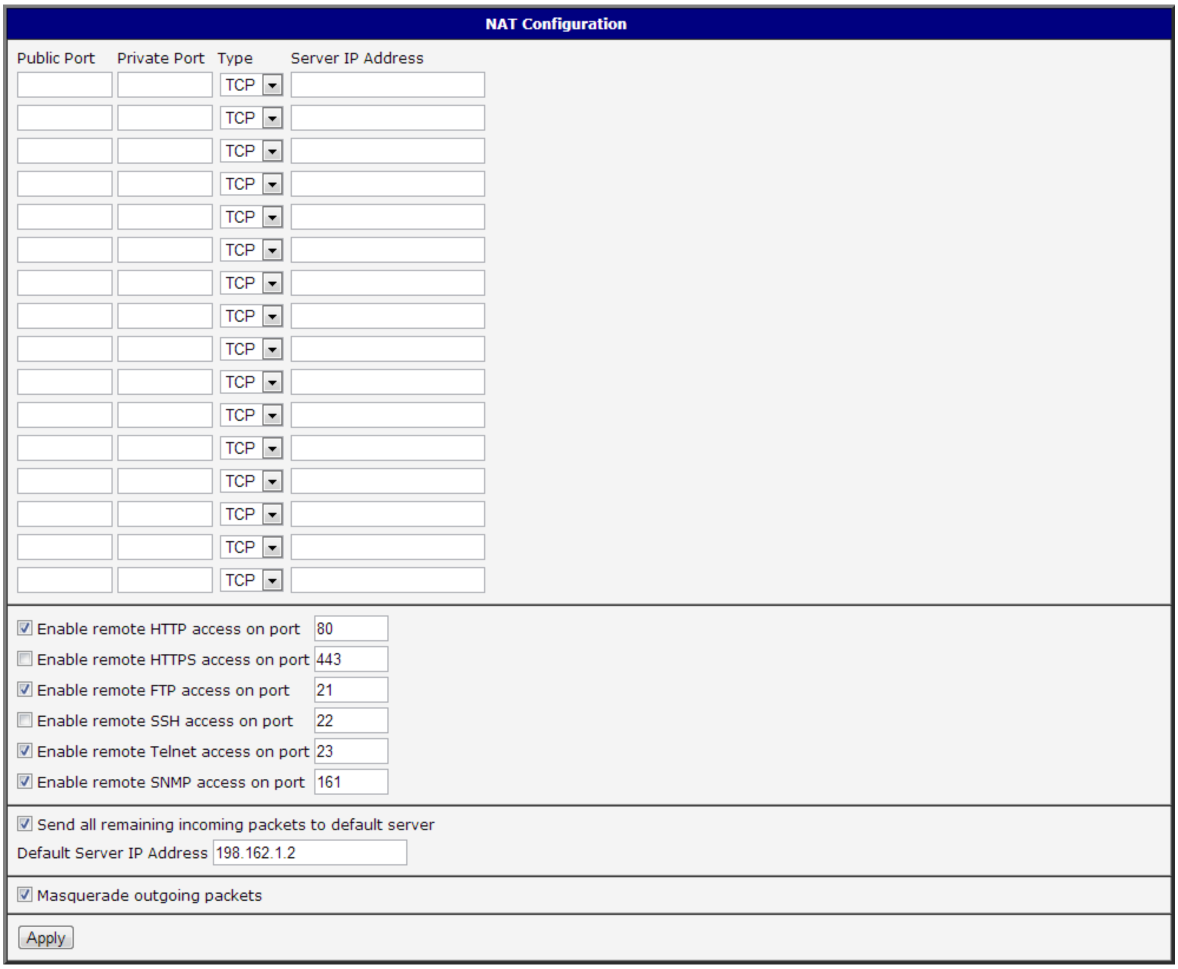


Figure 26: Topology of example NAT configuration 1



NAT Configuration

Public Port	Private Port	Type	Server IP Address
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☑ Enable remote HTTP access on port 80
☐ Enable remote HTTPS access on port 443
☑ Enable remote FTP access on port 21
☐ Enable remote SSH access on port 22
☑ Enable remote Telnet access on port 23
☑ Enable remote SNMP access on port 161

☑ Send all remaining incoming packets to default server
Default Server IP Address 198.162.1.2

☑ Masquerade outgoing packets

Figure 27: Example NAT configuration 1

In these configurations it is important to have marked choice of *Send all remaining incoming packets it default server*, IP address in this case is the address of the device behind the router. Connected equipment behind the router must have set *Default Gateway* on the router. Connected device replies, while PING on IP address of SIM card.

Example of the configuration with more connected equipment:

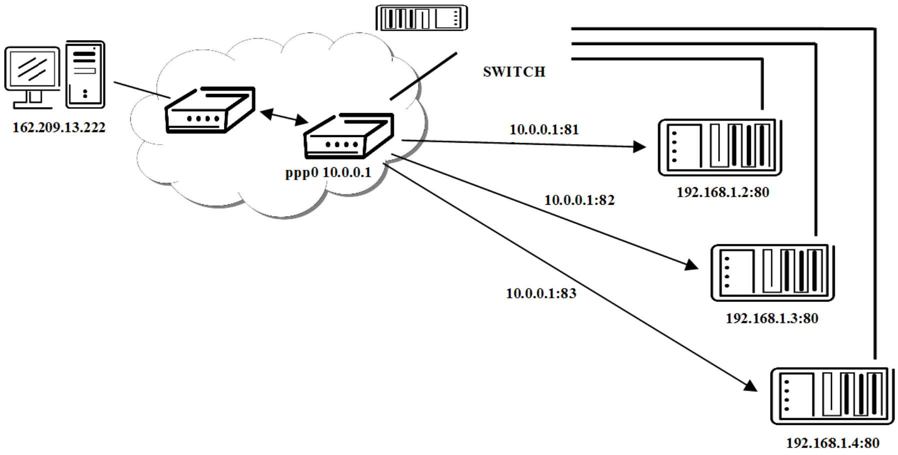
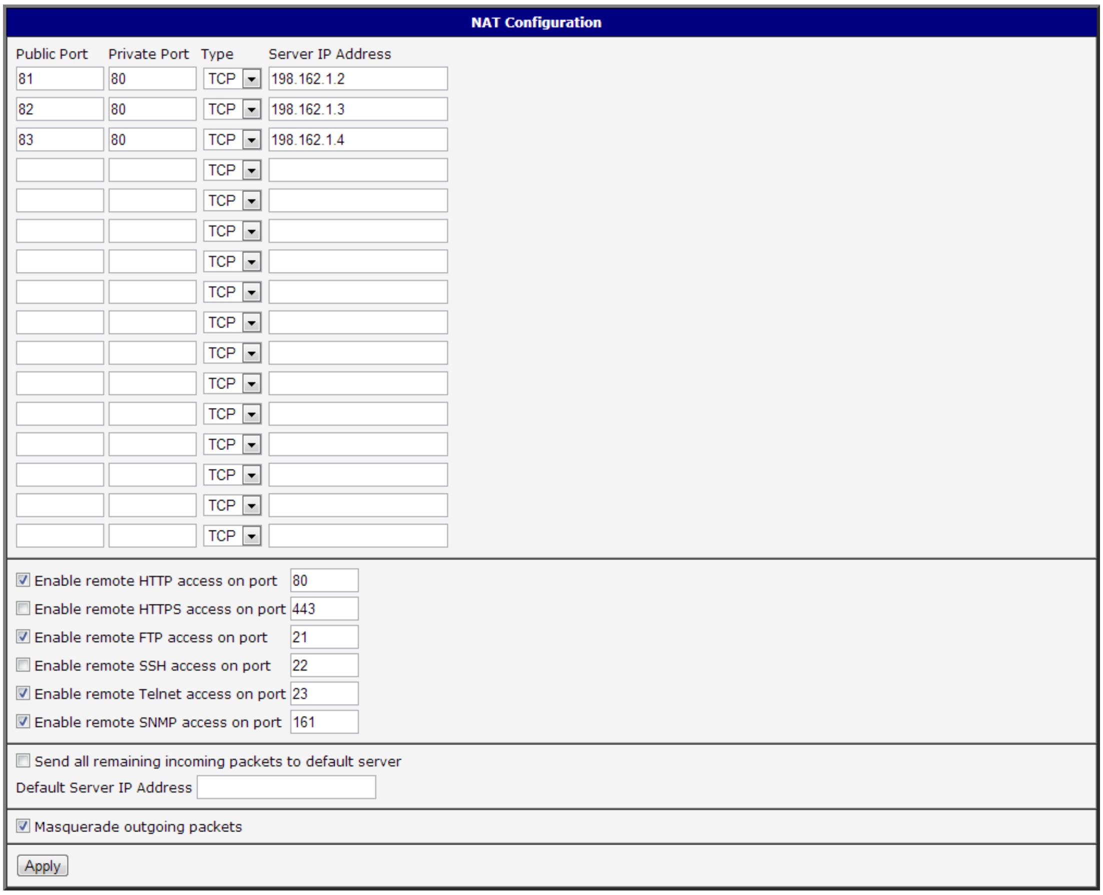


Figure 28: Topology of example NAT configuration 2



NAT Configuration

Public Port	Private Port	Type	Server IP Address
81	80	TCP	198.162.1.2
82	80	TCP	198.162.1.3
83	80	TCP	198.162.1.4
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☑ Enable remote HTTP access on port 80
□ Enable remote HTTPS access on port 443
☑ Enable remote FTP access on port 21
□ Enable remote SSH access on port 22
☑ Enable remote Telnet access on port 23
☑ Enable remote SNMP access on port 161

□ Send all remaining incoming packets to default server
Default Server IP Address

☑ Masquerade outgoing packets

Figure 29: Example NAT configuration 2

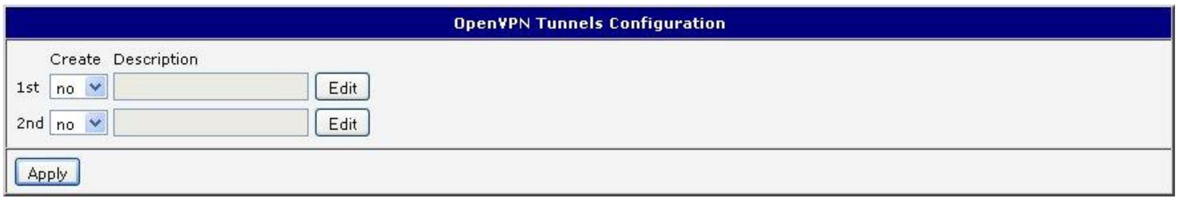
In this configuration equipment wired behind the router defines the address *Server IP Address*. The router replies, while PING on address of SIM card. Access on web interface of the equipment behind the router is possible by the help of Port Forwarding, when behind IP address of SIM is indicating public port of equipment on which we want to come up. At demand on port 80 it is surveyed singles outer ports (Public port), there this port isn't defined, therefore at check selection Enable remote http access it automatically opens the web interface router. If this choice isn't selected and is selected volition Send all remaining incoming packets to the default server fulfill oneself connection on induction IP address. If it is not selected selection *Send all remaining incoming packets to default server* and *Default server IP address* then connection requests a failure.

1.16 OpenVPN tunnel configuration

OpenVPN tunnel configuration can be called up by option *OpenVPN* item in the menu. OpenVPN tunnel allows protected connection of two networks LAN to the one which looks like one homogenous. In the *OpenVPN Tunnels Configuration* window are two rows, each row for one configured OpenVPN tunnel.

Item	Description
Create	This item enables the individual tunnels.
Description	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration OpenVPN tunnel.

Table 29: Overview OpenVPN tunnels



OpenVPN Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit

Figure 30: OpenVPN tunnels configuration

Item	Description
Description	Description of tunnel.
Protocol	Protocol, by which the tunnel will communicate. • UDP – OpenVPN will communicate using UDP. • TCP server – OpenVPN will communicate using TCP in server mode.

Continued on next page

Continued from previous page

Item	Description
	• TCP client – OpenVPN will communicate using TCP in client mode.
UDP/TCP port	Port, by which the tunnel will communicate.
Remote IP Address	IP address of the opposite side of the tunnel. Can be used domain name.
Remote Subnet	Network IP address of the opposite side of the tunnel.
Remote Subnet Mask	Subnet mask of the opposite side of the tunnel.
Redirect Gateway	By this parameter is possible to redirect all traffic on Ethernet.
Local Interface IP Address	IP address of the local side of tunnel.
Remote Interface IP Address	IP address of interface local side of tunnel.
Ping Interval	This parameter defines the time period after which router sends a message to opposite side of tunnel, for check the existence of the tunnel.
Ping Timeout	*Ping Timeout* waits on message from off-side tunnel. For OpenVPN tunnel right verifies parameter *Ping Timeout* has to be bigger than *Ping Interval*.
Renegotiate Interval	Sets renegotiate period (reauthorization) of the OpenVPN tunnel. This parameter is possible to set only at username/password authentication or at X.509 certificate using. After this time period, the router changes the encryption tunnel to ensure the continued safety of the tunnel.
Max Fragment Size	By parameter *Max Fragment Size* it is possible to define maximum sending packet size.
Compression	Sending data is possible compress • none – No compression is used. • LZO – Are used lossless LZO compressions. Compression has to be on both tunnel ends.
NAT Rules	By parameter NAT Rules it is possible to apply set NAT rules to OpenVPN tunnel. • not applied – NAT rules to OpenVPN is not applied. • applied – NAT rules to OpenVPN is applied.
Authenticate Mode	This parameter can be set authentication mode. • none – is used any authentication mode

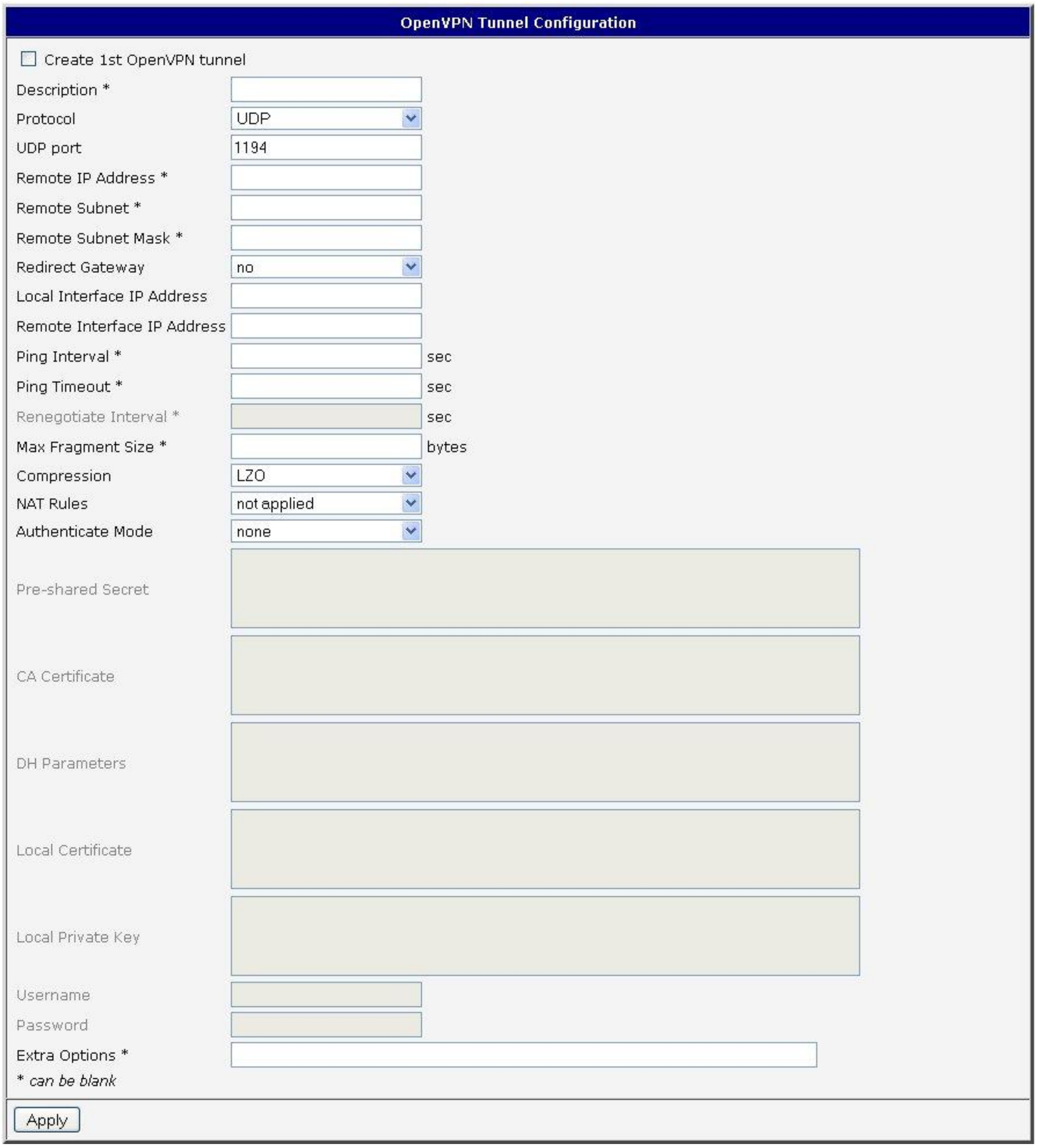
Continued on next page

Continued from previous page

Item	Description
	• Pre-shared secret – enables authentication using Pre-shared secret. This authentication set shared key for both off-side tunnel • Username/password – enables authentication using CA Certificate, Username and Password • X.509 Certificate (multiclient) – enables authentication by CA Certificate, Local Certificate and Local Private Key • X.509 Certificate (client) – enables authentication by CA Certificate, Local Certificate and Local Private Key • X.509 Certificate (server) - enables authentication by CA Certificate, Local Certificate and Local Private Key
Pre-shared Secret	Authentication using Pre-shared secret can be used in all offered authentication mode.
CA Certificate	This authentication certificate can be used in authentication mode Username/password and X.509 certificate.
DH Parameters	Protocol for exchange key DH parameters can be used in authentication mode X.509 server.
Local Certificate	This authentication certificate can be used in authentication mode X.509 certificate.
Local Private Key	Local private key can be used in authentication mode X.509 certificate.
Username	Authentication using a login name and password authentication can be used in the Authenticate Mode Username/Password.
Password	Authentication using a login name and password authentication can be used in the Authenticate Mode Username/Password.
Extra Options	By the help of parameter *Extra Options* it is possible to define additional parameters of the OpenVPN tunnel, for example DHCP options etc.

Table 30: OpenVPN tunnels configuration

The changes in settings will apply after pressing the *Apply* button.



OpenVPN Tunnel Configuration

□ Create 1st OpenVPN tunnel

Description *		
Protocol	UDP	
UDP port	1194	
Remote IP Address *		
Remote Subnet *		
Remote Subnet Mask *		
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *		sec
Ping Timeout *		sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	none	
Pre-shared Secret		
CA Certificate		
DH Parameters		
Local Certificate		
Local Private Key		
Username		
Password		
Extra Options *		

* *can be blank*

Figure 31: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

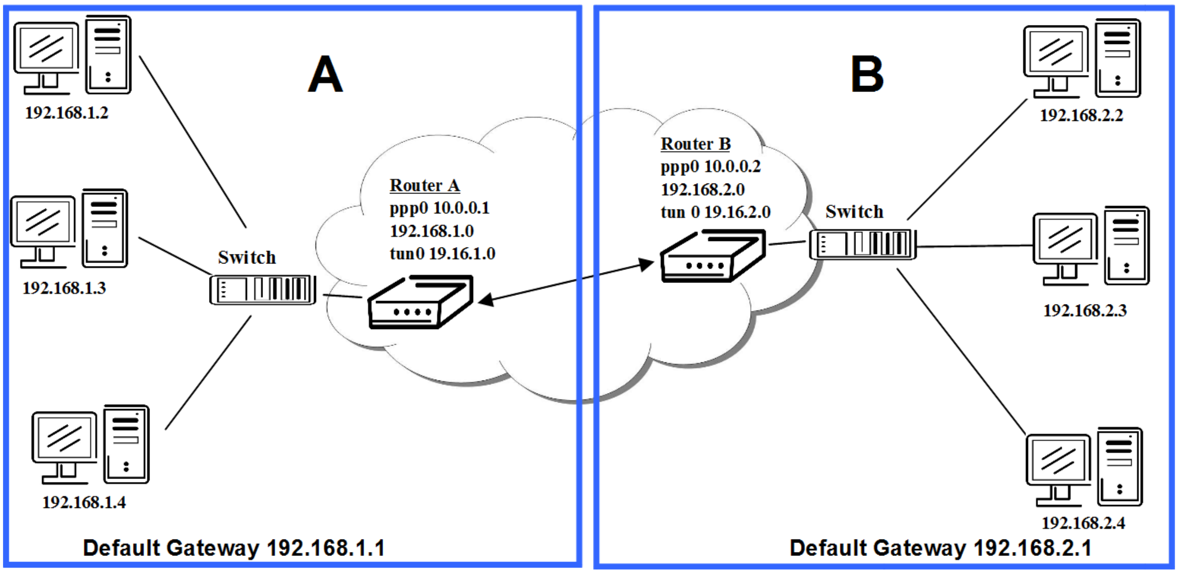


Figure 32: Topology of example OpenVPN configuration

OpenVPN tunnel configuration:

Configuration	A	B
Protocol	UDP	UDP
UDP Port	1194	1194
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.18.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Table 31: Example OpenVPN configuration

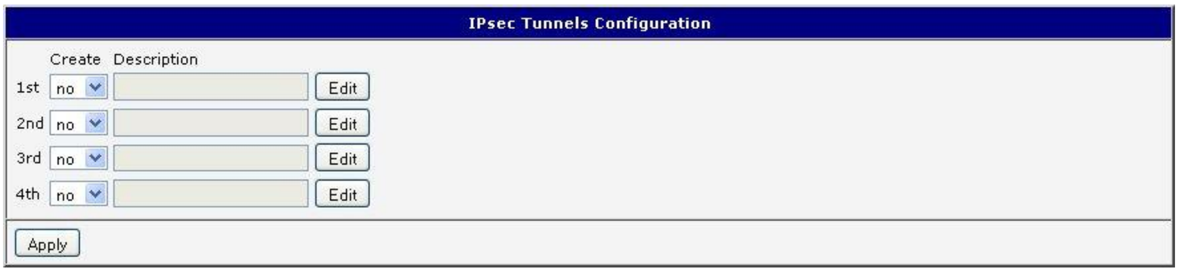
Examples of different options for configuration and authentication of OpenVPN can be found in the configuration manual OpenVPN tunnel.

1.17 IPSec tunnel configuration

IPsec tunnel configuration can be called up by option *IPsec* item in the menu. IPsec tunnel allows protected (encrypted) connection of two networks LAN to the one which looks like one homogenous. In the *IPsec Tunnels Configuration* window are four rows, each row for one configured one IPSec tunnel.

Item	Description
Create	This item enables the individual tunnels.
Description	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration IPsec tunnel.

Table 32: Overview IPsec tunnels



IPsec Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit
3rd	no		Edit
4th	no		Edit

Figure 33: IPsec tunnels configuration

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address of opposite side tunnel. Can be used domain main.
Remote ID	Identification of opposite side tunnel. Parameters ID contain two parts: hostname and domain-name.
Remote Subnet	Address nets behind off – side tunnel
Remote Subnet Mask	Subnet mask behind off – side tunnel
Local ID	Identification of local side. Parameters ID contain two parts: hostname and domain-name.
Local Subnet	Local subnet address
Local subnet mask	Local subnet mask
Encapsulation Mode	IPsec mode – you can choose tunnel or transport
NAT traversal	If address translation between two end points of the IPsec tunnel is used, it needs to allow NAT Traversal

Continued on next page

Continued from previous page

Item	Description
IKE Mode	Defines mode for establishing connection (*main* or *aggressive*). If the *aggressive* mode is selected, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5.
IKE Algorithm	Way of algorithm selection: • *auto* – encryption and hash alg. are selected automatically • *manual* – encryption and hash alg. are defined by the user
IKE Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256
IKE Hash	Hash algorithm – MD5 or SHA1
IKE DH Group	Diffie-Hellman groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key. Group with higher number provides more security, but requires more processing time.
ESP Algorithm	Way of algorithm selection: • *auto* – encryption and hash alg. are selected automatically • *manual* – encryption and hash alg. are defined by the user
ESP Encryption	Encryption algorithm – DES, 3DES, AES128, AES192, AES256
ESP Hash	Hash algorithm – MD5 or SHA1
PFS	Ensures that derived session keys are not compromised if one of the private keys is compromised in the future
PFS DH Group	Diffie-Hellman group number (see *IKE DH Group*)
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before connection expiry should attempt to negotiate a replacement begin. The maximum value must be less than half the parameters IKE and Key Lifetime.
Rekey Fuzz	Specifies the maximum percentage by which should be randomly increased to randomize re-keying intervals
DPD Delay	Defines time after which is made IPsec tunnel verification
DPD Timeout	By parameter DPD Timeout is set timeout of the answer
Authenticate Mode	By this parameter can be set authentication: • Pre-shared key – shared key for both off-side tunnel. • X.509 Certificate – allows X.509 certification in multiclient mode

Continued on next page

Continued from previous page

Item	Description
Pre-shared Key	Sharable key for both parties tunnel.
CA Certificate	This certificate is necessary to insert Authentication mode x.509.
Remote Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Private Key	This private key is necessary to insert Authentication mode x.509.
Local Passphrase	This Local Passphrase is necessary to insert Authentication mode x.509.
Extra Options	Use this parameter to define additional parameters of the IPsec tunnel, for example secure parameters etc.

Table 33: OpenVPN tunnels configuration

The certificates and private keys have to be in PEM format. As certificate it is possible to use only certificate which has start and stop tag certificate.

Random time, after which it will re-exchange of new keys are defined:

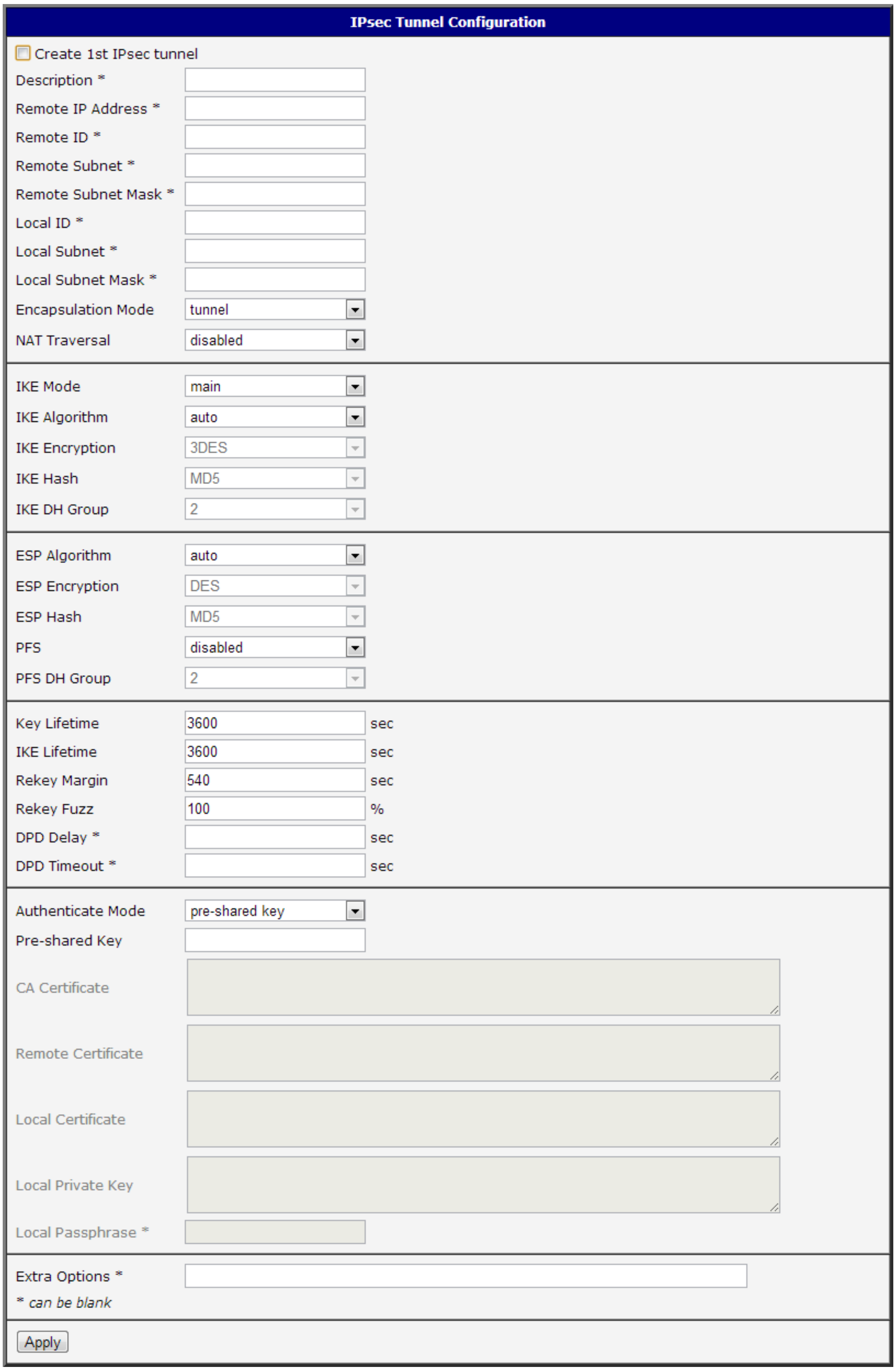
*Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))*

By default, the repeated exchange of keys held in the time range:

- Minimal time: 1h - (9m + 9m) = 42m
- Maximal time: 1h - (9m + 0m) = 51m

When setting the times for key exchange is recommended to leave the default setting in which tunnel has guaranteed security. When set higher time, tunnel has smaller operating costs and smaller the safety. Conversely, reducing the time, tunnel has higher operating costs and higher safety of the tunnel.

The changes in settings will apply after pressing the *Apply* button.



IPsec Tunnel Configuration

□ Create 1st IPsec tunnel

Description *		
Remote IP Address *		
Remote ID *		
Remote Subnet *		
Remote Subnet Mask *		
Local ID *		
Local Subnet *		
Local Subnet Mask *		
Encapsulation Mode	tunnel	
NAT Traversal	disabled	
IKE Mode	main	
IKE Algorithm	auto	
IKE Encryption	3DES	
IKE Hash	MD5	
IKE DH Group	2	
ESP Algorithm	auto	
ESP Encryption	DES	
ESP Hash	MD5	
PFS	disabled	
PFS DH Group	2	
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
DPD Delay *		sec
DPD Timeout *		sec
Authenticate Mode	pre-shared key	
Pre-shared Key		
CA Certificate		
Remote Certificate		
Local Certificate		
Local Private Key		
Local Passphrase *		
Extra Options *		

* *can be blank*

Figure 34: IPsec tunnels configuration

Example of the IPSec Tunnel configuration:

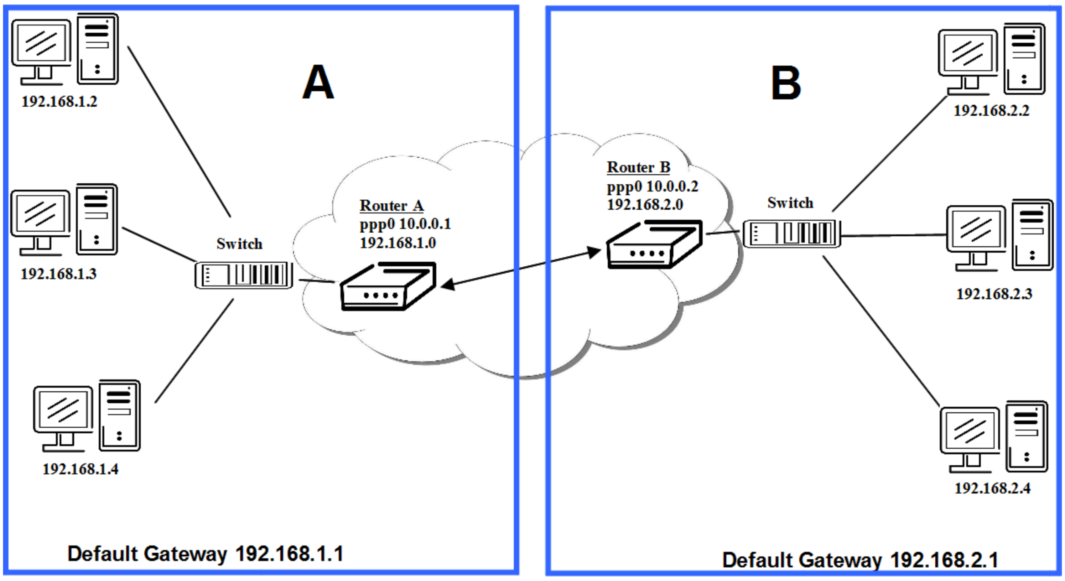


Figure 35: Topology of example IPsec configuration

IPsec tunnel configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mas:	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Table 34: Example IPsec configuration

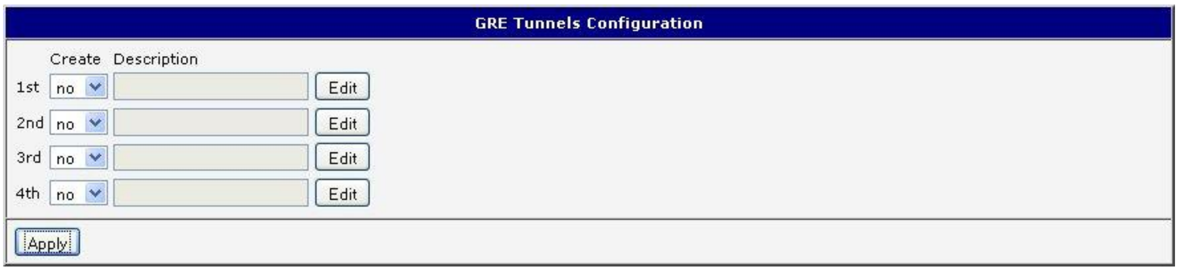
Examples of different options for configuration and authentication of IPsec can be found in the configuration manual IPsec tunnel.

1.18 GRE tunnels configuration

To enter the GRE tunnels configuration, select the *GRE* menu item. The GRE tunnel is used for connection of two networks to one that appears as one homogenous. It is possible to configure up to four GRE tunnels. In the *GRE Tunnels Configuration* window are four rows, each row for one configured GRE tunnel.

Item	Description
Create	Enables the individual tunnels.
Description	Displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration GRE tunnel.

Table 35: Overview GRE tunnels



GRE Tunnels Configuration

	Create	Description	
1st	no		Edit
2nd	no		Edit
3rd	no		Edit
4th	no		Edit

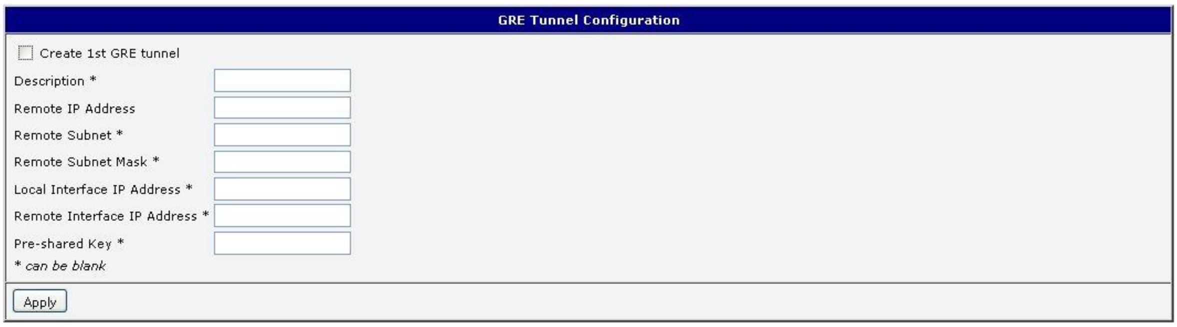
Figure 36: GRE tunnels configuration

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address of the remote side of the tunnel
Local Interface IP Address	IP address of the local side of the tunnel
Remote Interface IP Address	IP address of the remote side of the tunnel
Remote Subnet	IP address of the network behind the remote side of the tunnel
Remote Subnet Mask	Mask of the network behind the remote side of the tunnel
Pre-shared Key	An optional value that defines the 32 bit shared key, through which the filtered data through the tunnel. This key must be defined on both routers as same, otherwise the router will drop received packets. Using this key, the data do not provide a tunnel through.

Table 36: GRE tunnel configuration

Attention, GRE tunnel doesn't connect itself via NAT.

The changes in settings will apply after pressing the *Apply* button.



GRE Tunnel Configuration

□ Create 1st GRE tunnel

Description *
Remote IP Address
Remote Subnet *
Remote Subnet Mask *
Local Interface IP Address *
Remote Interface IP Address *
Pre-shared Key *
can be blank

Figure 37: GRE tunnel configuration

Example of the GRE Tunnel configuration:

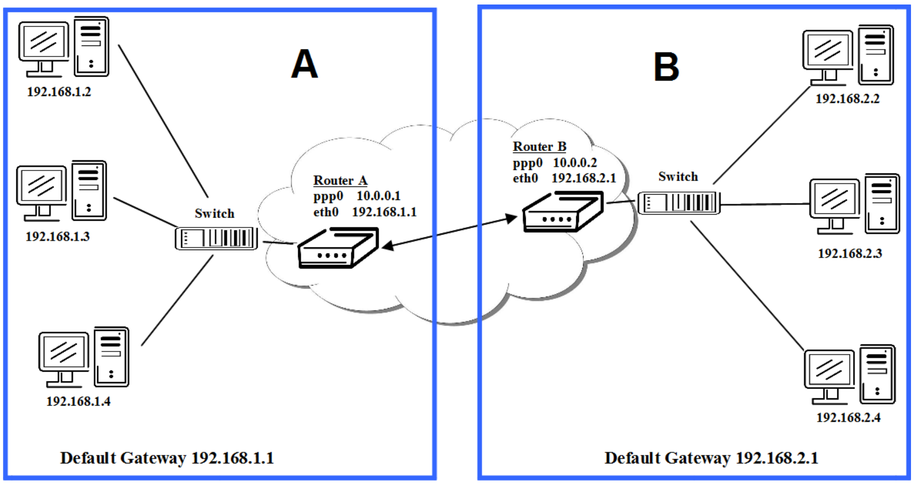


Figure 38: Topology of GRE tunnel configuration

GRE tunnel Configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Table 37: Example GRE tunnel configuration

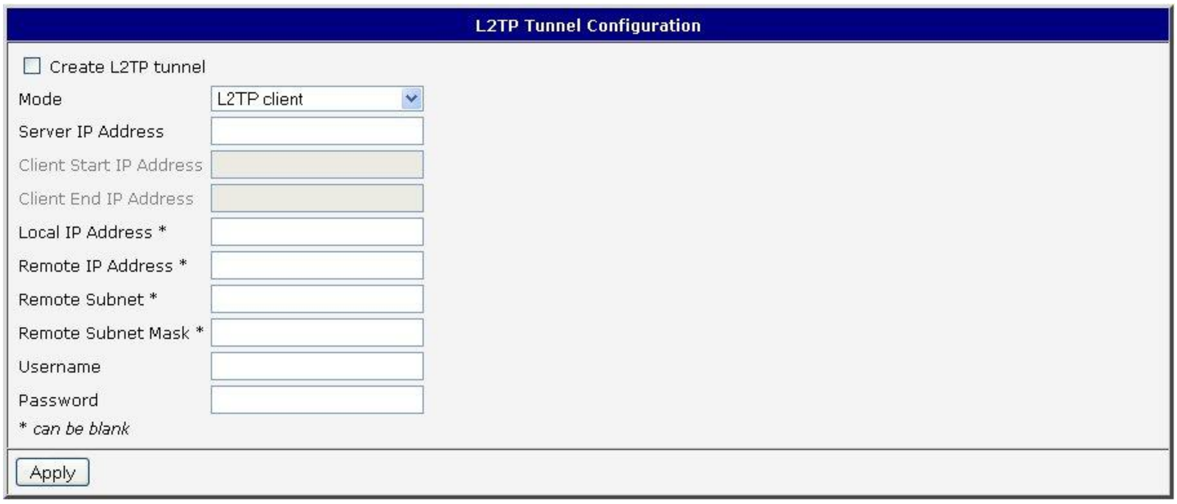
1.19 L2TP tunnel configuration

To enter the L2TP tunnels configuration, select the L2TP menu item. L2TP tunnel allows protected connection by password of two networks LAN to the one which it looks like one homogenous. The tunnels are active after selecting Create L2TP tunnel.

Item	Description
Mode	L2TP tunnel mode on the router side: • L2TP server – in the case of a server must define the start and end IP address range offered by the server • L2TP client – in case of client must define the IP address of the server
Server IP Address	IP address of server
Client Start IP Address	Start IP address in range, which is offered by server to clients
Client End IP Address	End IP address in range, which is offered by server to clients
Local IP Address	IP address of the local side of the tunnel
Remote IP Address	IP address of the remote side of the tunnel
Remote Subnet	Address of the network behind the remote side of the tunnel
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
Username	Username for login to L2TP tunnel
Password	Password for login to L2TP tunnel

Table 38: L2TP tunnel configuration

The changes in settings will apply after pressing the *Apply* button.



L2TP Tunnel Configuration

□ Create L2TP tunnel

Mode	L2TP client
Server IP Address	
Client Start IP Address	
Client End IP Address	
Local IP Address *	
Remote IP Address *	
Remote Subnet *	
Remote Subnet Mask *	
Username	
Password	

* *can be blank*

Figure 39: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

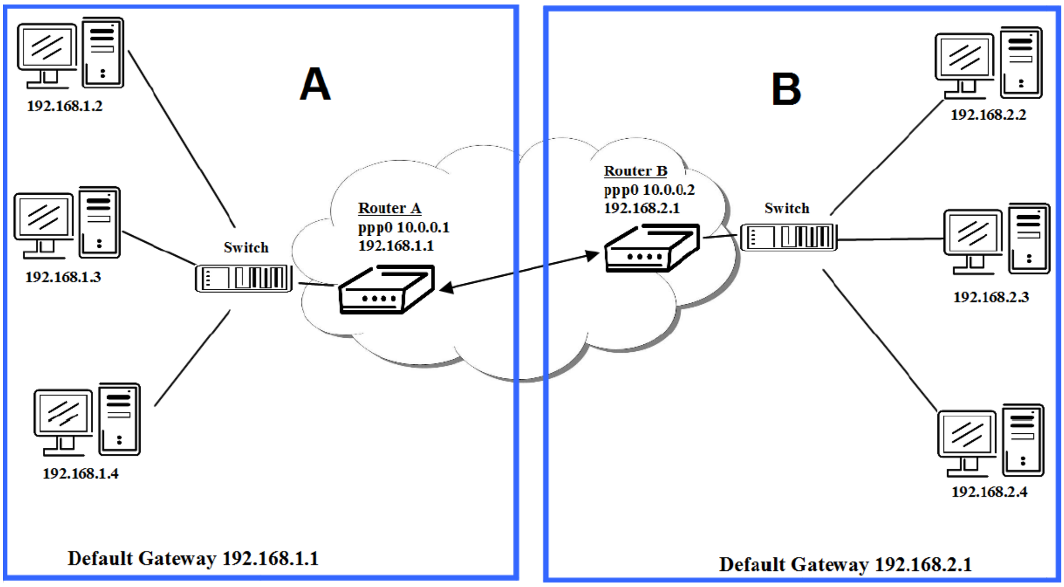


Figure 40: Topology of example L2TP tunnel configuration

Configuration of the L2TP tunnel:

Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.1.2	—
Client End IP Address	192.168.1.254	—
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 39: Example L2TP tunel configuration

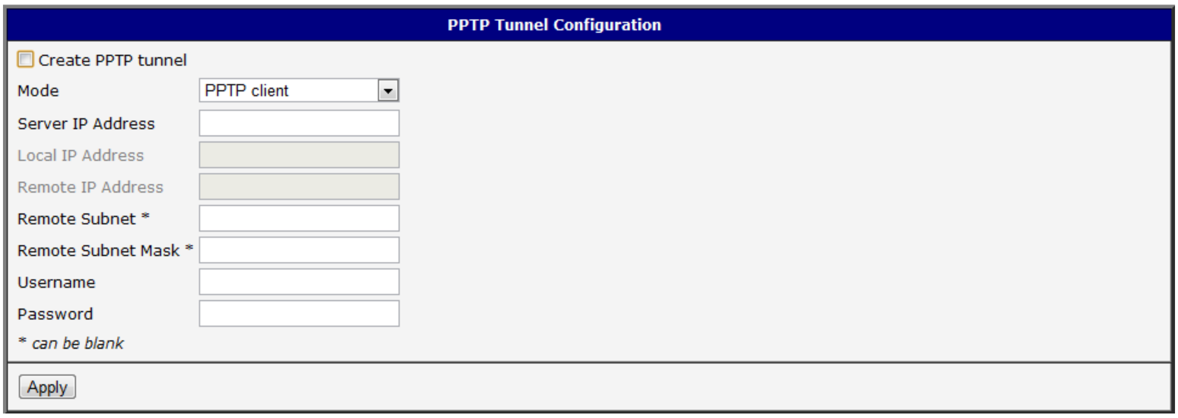
1.20 PPTP tunnel configuration

To enter the PPTP tunnels configuration, select the *PPTP* menu item. PPTP tunnel allows protected connection by password of two networks LAN to the one which it looks like one homogenous. It is a similar method of VPN execution as L2TP. The tunnels are active after selecting *Create PPTP tunnel*.

Item	Description
Mode	PPTP tunnel mode on the router side: ● PPTP server – in the case of a server must define the start and end IP address range offered by the server ● PPTP client – in case of client must define the IP address of the server
Server IP Address	IP address of server
Local IP Address	IP address of the local side of the tunnel
Remote IP Address	IP address of the remote side of the tunnel
Remote Subnet	Address of the network behind the remote side of the tunnel
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
Username	Username for login to PPTP tunnel
Password	Password for login to PPTP tunnel

Table 40: PPTP tunnel configuration

The changes in settings will apply after pressing the *Apply* button.



PPTP Tunnel Configuration

□ Create PPTP tunnel

Mode	PPTP client
Server IP Address	
Local IP Address	
Remote IP Address	
Remote Subnet *	
Remote Subnet Mask *	
Username	
Password	

* *can be blank*

Figure 41: PPTP tunnel configuration

Example of the PPTP Tunnel configuration:

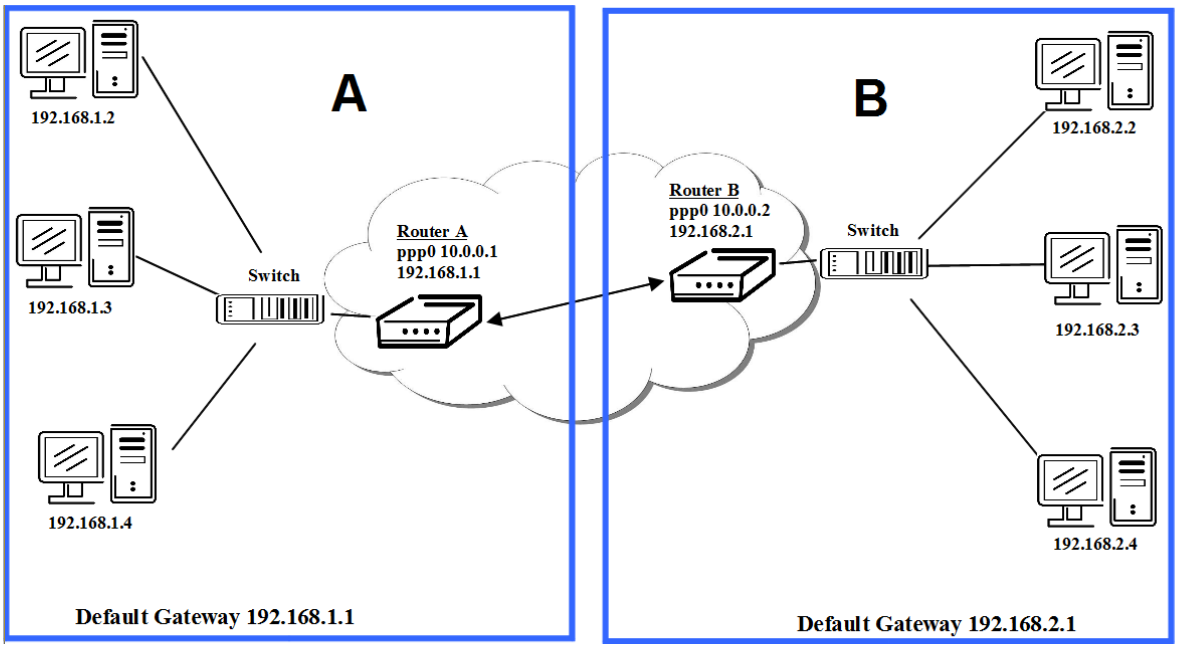


Figure 42: Topology of example PPTP tunnel configuration

Configuration of the PPTP tunnel:

Configuration	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 41: Example PPTP tunel configuration

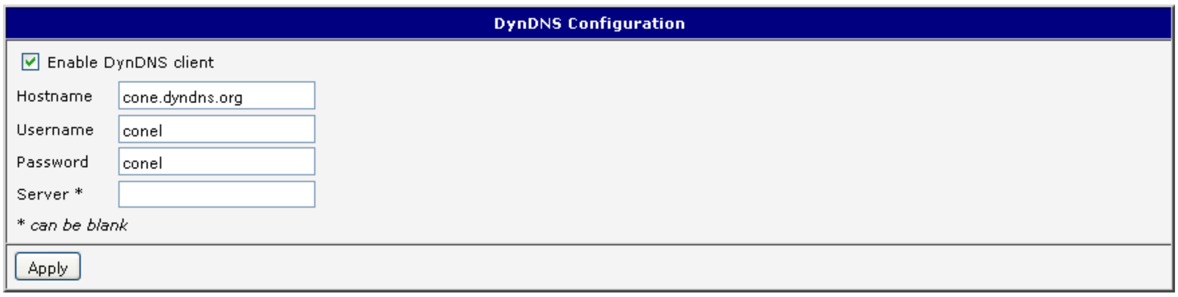
1.21 DynDNS client configuration

DynDNS client Configuration can be called up by option *DynDNS* item in the menu. In the window can be defined a third order domain registered on server www.dyndns.org.

Item	Description
Hostname	Third order domain registered on server www.dyndns.org
Username	Username for login to DynDNS server
Password	Password for login to DynDNS server
Server	If you want to use another DynDNS service than www.dyndns.org, then enter the update server service to this item. If this item is left blank, it uses the default server members.dyndns.org.

Table 42: DynDNS configuration

Example of the DynDNS client configuration with domain conel.dyndns.org:


DynDNS Configuration

☑ Enable DynDNS client

Hostname	cone.dyndns.org
Username	conel
Password	conel
Server *	

* can be blank

Figure 43: Example of DynDNS configuration

1.22 NTP client configuration

NTP client Configuration can be called up by option *NTP* item in the menu. NTP (Network Time Protocol) allows set the exact time to the router from the servers, which provide the exact time on the network.

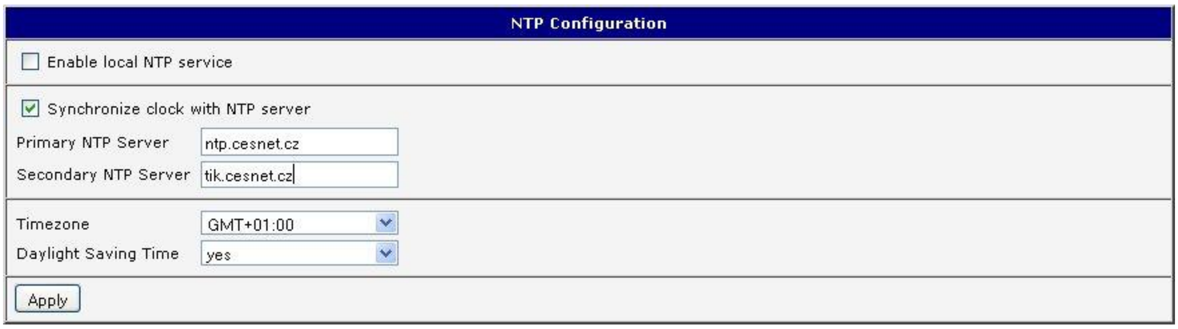
By parameter *Enable local NTP service* router is set to a mode in which it operates as an NTP server for other devices in the LAN behind the router.

By parameter *Enable local NTP service* it is possible to set the router in mode, that it can serve as NTP server for other devices.

Item	Description
Primary NTP Server Address	IP or domain address primary NTP server.
Secondary NTP Server Address	IP or domain address secondary NTP server.
Timezone	By this parameter it is possible to set the time zone of the router
Daylight Saving Time	By this parameter is possible to define time shift: • No – time shift is disabled • Yes – time shift is allowed

Table 43: NTP configuration

Example of the NTP conf. with set primary (ntp.cesnet.cz) and secondary (tik.cesnet.cz) NTP server and with daylight saving time:



NTP Configuration

□ Enable local NTP service

☑ Synchronize clock with NTP server

Primary NTP Server: ntp.cesnet.cz

Secondary NTP Server: tik.cesnet.cz

Timezone: GMT+01:00

Daylight Saving Time: yes

Figure 44: Example of NTP configuration

1.23 SNMP configuration

To enter the *SNMP configuration* it is possible with SNMP agent v1/v2 or v3 configuration which sends information about the router, eventually about the status of the expansion port CNT or MBUS.

SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or end computers.

Item	Description
Name	Designation of the router.
Location	Placing of the router.
Contact	Person who manages the router together with information how to contact this person.

Table 44: SNMP agent configuration

Enabling SNMPv1/v2 is performed using the *Enable SNMPv1/v2 access* item. It is also necessary to define a password for access to the SNMP agent (*Community*).

The *Enable SNMPv3 access* item allows you to enable SNMPv3. Then you must define the following parameters:

Item	Description
Username	User name
Authentication	Encryption algorithm on the Authentication Protocol that is used to ensure the identity of users.
Authentication Password	Password used to generate the key used for authentication.
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol.

Table 45: SNMPv3 configuration

In addition, you can continue with this configuration:

- By choosing *Enable I/O extension* it is possible to monitor binary inputs I/O on the router.
- By choosing *Enable XC-CNT extension* it is possible to monitor the expansion port CNT inputs and outputs status.
- By choosing *Enable M-BUS extension* and enter the *Baudrate*, *Parity* and *Stop Bits* it is possible to monitor the meter status connected to the expansion port MBUS status.

Item	Description
Baudrate	Communication speed.
Parity	Control parity bit: • none – Data will be sent without parity. • even – Data will be sent with even parity. • odd – Data will be sent with odd parity.
Stop Bits	Number of stop bit.

Table 46: SNMP configuration (MBUS extension)

❗ Parameters Enable *XC-CNT extension* and *Enable M-BUS extension* can not be checked together.

By choosing *Enable reporting to supervisory system* and enter the *IP Address* and *Period* it is possible to send statistical information to the monitoring system R-SeeNet.

Item	Description
IP Address	IP address
Period	Period of sending statistical information (in minutes)

Table 47: SNMP configuration (R-SeeNet)

Every monitor value is uniquely identified by the help of number identifier *OID – Object Identifier*. For binary input and output the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Binary input BIN0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binary output OUT0 (values 0,1)

Table 48: Object identifier for binary input and output

For the expansion port CNT the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.1.1.0	Analogy input AN1 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogy input AN2 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Counter input CNT1 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Counter input CNT2 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binary input BIN1 (values 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binary input BIN2 (values 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binary input BIN3 (values 0,1)

Continued on next page

Continued from previous page

OID	Description
.1.3.6.1.4.1.30140.2.1.8.0	Binary input BIN4 (values 0,1)
.1.3.6.1.4.1.30140.2.1.9.0	Binary output OUT1 (values 0,1)

Table 49: Object identifier for CNT port

For the expansion port M-BUS the following range of OID is used:

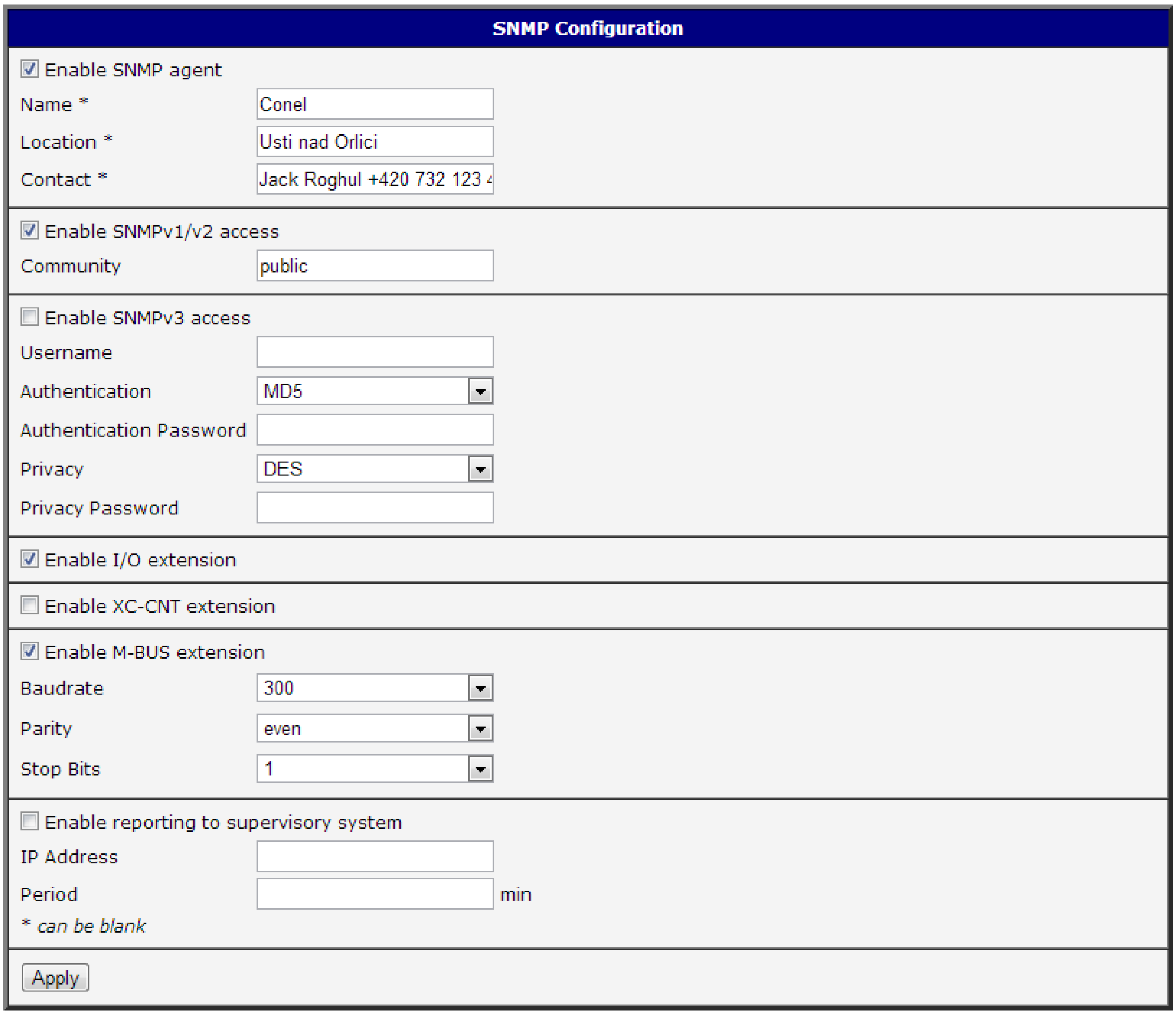
OID	Description
.1.3.6.1.4.1.30140.2.2.<address>.1.0	IdNumber – meter number
.1.3.6.1.4.1.30140.2.2.<address>.2.0	Manufacturer
.1.3.6.1.4.1.30140.2.2.<address>.3.0	Version – specified meter version
.1.3.6.1.4.1.30140.2.2.<address>.4.0	Medium – type of metered medium
.1.3.6.1.4.1.30140.2.2.<address>.5.0	Status – errors report
.1.3.6.1.4.1.30140.2.2.<address>.6.0	0. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.7.0	0. measured value
.1.3.6.1.4.1.30140.2.2.<address>.8.0	1. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.9.0	1. measured value
.1.3.6.1.4.1.30140.2.2.<address>.10.0	2. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.11.0	2. measured value
.1.3.6.1.4.1.30140.2.2.<address>.12.0	3. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.13.0	3. measured value
⋮	⋮
.1.3.6.1.4.1.30140.2.2.<address>.100.0	47. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.101.0	47. measured value

Table 50: Object identifier for M-BUS port

The meter address can be from range 0..254 when 254 is broadcast.

Since firmware 3.0.4 all v2 routers with board RB-v2-6 and newer provide information about internal temperature of device (OID 1.3.6.1.4.1.30140.3.3) and power voltage (OID 1.3.6.1.4.1.30140.3.4).

Example of SNMP settings and readout:



SNMP Configuration

☑ Enable SNMP agent

Name *	Conel
Location *	Usti nad Orlici
Contact *	Jack Roghul +420 732 123 4

☑ Enable SNMPv1/v2 access

Community	public

☐ Enable SNMPv3 access

Username	
Authentication	MD5
Authentication Password	
Privacy	DES
Privacy Password	

☑ Enable I/O extension

☐ Enable XC-CNT extension

☑ Enable M-BUS extension

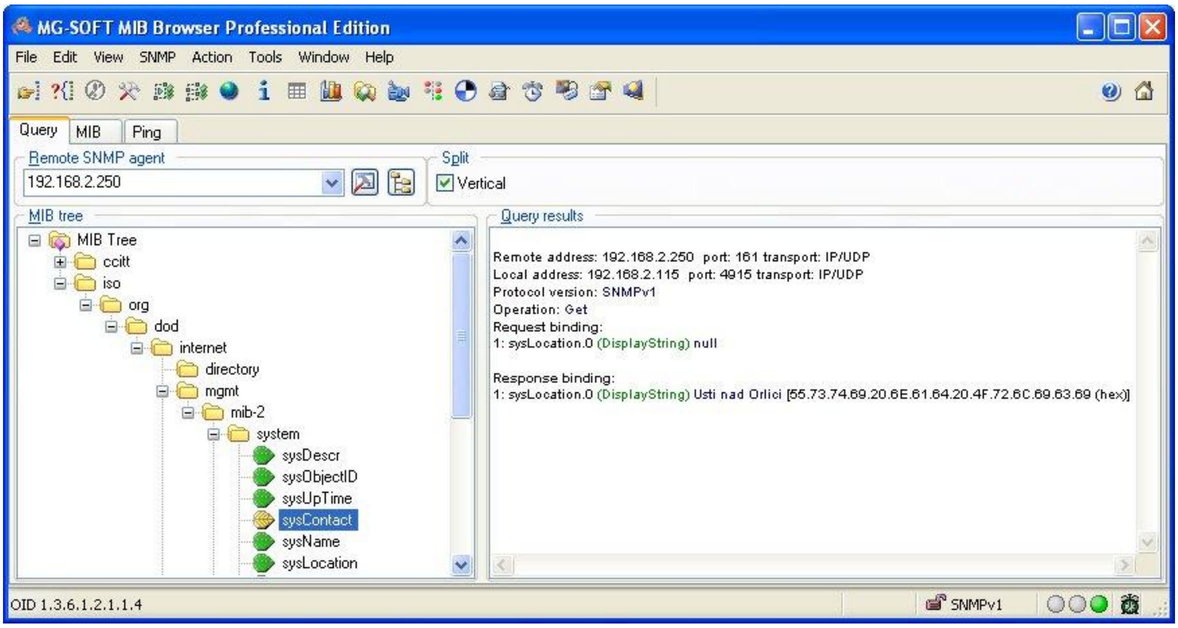
Baudrate	300
Parity	even
Stop Bits	1

☐ Enable reporting to supervisory system

IP Address	
Period	min

* *can be blank*

Figure 45: Example of SNMP configuration



Remote SNMP agent: 192.168.2.250

☑ Vertical

```
Remote address: 192.168.2.250  port: 161 transport: IP/UDP
Local address: 192.168.2.115  port: 4915 transport: IP/UDP
Protocol version: SNMPv1
Operation: Get
Request binding:
1: sysLocation.0 (DisplayString) null

Response binding:
1: sysLocation.0 (DisplayString) Usti nad Orlici [55.73.74.69.20.6E.61.64.20.4F.72.6C.69.63.69 (hex)]
```

OID 1.3.6.1.2.1.1.4

Figure 46: Example of the MIB browser

It is important to set the IP address of the SNMP agent (router) in field Remote SNMP agent. After enter the IP address is in a MIB tree part is possible show object identifier.

The path to objects is:

iso → org → dod → internet → private → enterprises → conel → protocols

The path to information about router is:

iso → org → dod → internet → mgmt → mib-2 → system

1.24 SMTP configuration

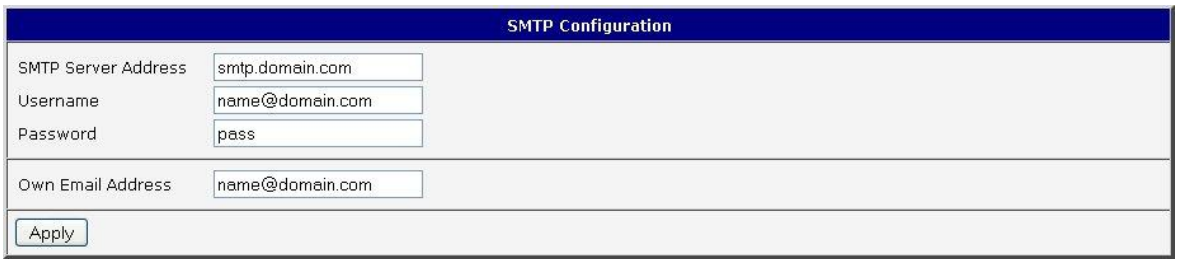
To enter the *SMTP* it is possible configure SMTP (Simple Mail Transfer Protocol) client, which is set by sending emails.

Item	Description
SMTP Server Address	IP or domain address of the mail server.
Username	Name to email account.
Password	Password to email account.
Own Email Address	Address of the sender.

Table 51: SMTP client configuration

Mobile operator can block other SMTP servers, then you can use only the SMTP server of operator.

Example settings SMTP client:



SMTP Configuration

SMTP Server Address	smtp.domain.com
Username	name@domain.com
Password	pass
Own Email Address	name@domain.com

Figure 47: SMTP configuration

E-mail can be send from the Startup script. This command is used to email with following parameters.

- -t receiver Email address
- -s subject
- -m message
- -a appendix
- -r number of attempts to send email (default set 2 attempts)

Commands and parameters can be entered only in lowercase.

Example to send email:

email –t name@domain.com –s "subject" –m "message" –a c:\directory\abc.doc –r 5

This command sends e-mail to address *jack@google.com* with the subject *"subject"*, body message *"message"* and annex *"abc.doc"* right from the directory c:\directory\and 5 attempts to send.

1.25 SMS configuration

For industrial router XR5i v2 is not available SMS Configuration item.

SMS Configuration can be called up by option *SMS* item in the menu. SMS configuration defines the options for sending SMS messages from the router at different defined events and states of the router. In the first part of window it configuration send SMS.

Item	Description
Send SMS on power up	Automatic sending of SMS messages after power up.
Send SMS on connect to mobile network	Automatic sending SMS message after connection to mobile network.
Send SMS on disconnect to mobile network	Automatic sending SMS message after disconnection to mobile network.
Send SMS when datalimit exceeded	Automatic sending SMS message after datalimit exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Automatic sending SMS message after binary input on I/O port (BIN0) is active. Text of message is intended parameter BIN0.
Send SMS when binary input on expansion port (BIN1 – BIN4) is active	Automatic sending SMS message after binary input on expansion port (BIN1 – BIN4) is active. Text of message is intended parameter BIN1 – BIN4.
Add timestamp to SMS	Adds time stamp to sent SMS messages. This stamp has a fixed format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Telephone numbers for sending automatically generated SMS.
Phone Number 2	Telephone numbers for sending automatically generated SMS.
Phone Number 3	Telephone numbers for sending automatically generated SMS.
Unit ID	The name of the router that will be sent in an SMS.
BIN0 – SMS	SMS text messages when activate the binary input on the router.
BIN1 – SMS	SMS text messages when activate the binary input on the expansion port.
BIN2 – SMS	SMS text messages when activate the binary input on the router.
BIN3 – SMS	SMS text messages when activate the binary input on the router.

Continued on next page

Continued from previous page

Item	Description
BIN4 – SMS	SMS text messages when activate the binary input on the router.

Table 52: Send SMS configuration

In the second part of the window it is possible to set function *Enable remote control via SMS*. After this it is possible to establish and close connection by SMS message.

Item	Description
Phone Number 1	This control can be configured for up to three numbers. If is set *Enable remote control via SMS*, all incoming SMS are processed and deleted. In the default settings this parameter is turned on.
Phone Number 2	This control can be configured for up to three numbers. If is set *Enable remote control via SMS*, all incoming SMS are processed and deleted. In the default settings this parameter is turned on.
Phone Number 3	This control can be configured for up to three numbers. If is set *Enable remote control via SMS*, all incoming SMS are processed and deleted. In the default settings this parameter is turned on.

Table 53: Control via SMS configuration

If no phone number is filled in, then it is possible to restart the router with the help of SMS in the form of Reboot from any phone number. While filling of one, two or three numbers it is possible to control the router with the help of an SMS sent only from these numbers. While filling of sign "*" it is possible control the router with the help of an SMS sent from every numbers.

Control SMS message doesn't change the router configuration. If the router is switched to offline mode by the SMS message the router will be in this mode up to next restart. This behavior is the same for all control SMS messages.

It is possible to send controls SMS in the form:

SMS	Description
go online sim 1	Switch to SIM1 card
go online sim 2	Switch to SIM2 card
go online	Switch router in online mode
go offline	connection termination
set out0=0	Set output I/O connector on 0
set out0=1	Set output I/O connector on 1

Continued on next page

Continued from previous page

SMS	Description
set out1=0	Set output expansion port XC-CNT on 0
set out1=1	Set output expansion port XC-CNT on 1
set profile std	Set standard profile
set profile alt1	Set alternative profile 1
set profile alt2	Set alternative profile 2
set profile alt3	Set alternative profile 3
reboot	Router reboot
get ip	Router send answer with IP address SIM card

Table 54: Control SMS

By choosing *Enable AT-SMS protocol on expansion port 1* and *Baudrate* it is possible to send/receive an SMS on the serial Port 1.

Item	Description
Baudrate	Communication speed expansion port 1

Table 55: Send SMS on serial PORT1 configuration

By choosing *Enable AT-SMS protocol on expansion port 2* and *Baudrate* it is possible to send/receive an SMS on the serial Port 2.

Item	Description
Baudrate	Communication speed expansion port 2

Table 56: Send SMS on serial PORT2 configuration

By choosing *Enable AT-SMS protocol on TCP port* and enter the *TCP port* it is possible to send/receive an SMS on the TCP port. SMS messages are sent by the help of a standard AT commands.

Item	Description
TCP Port	TCP port on which will be allowed to send/receive SMS messages.

Table 57: Send SMS on ethernet PORT1 configuration

1.25.1 Send SMS

After establishing connection with the router via serial interface or Ethernet, it is possible to use AT commands for work with SMS messages.

The following table only lists the commands that are supported by Conel's routers. For other AT commands is always sent *OK* response. There is no support for treatment of complex AT commands, so in such a case router sends *ERROR* response.

AT Command	Description
AT+CGMI	Returns the manufacturer specific identity
AT+CGMM	Returns the manufacturer specific model identity
AT+CGMR	Returns the manufacturer specific model revision identity
AT+CGPADDR	Displays the IP address of the ppp0 interface
AT+CGSN	Returns the product serial number
AT+CIMI	Returns the International Mobile Subscriber Identity number (IMSI)
AT+CMGD	Deletes a message from the location
AT+CMGF	Sets the presentation format of short messages
AT+CMGL	Lists messages of a certain status from a message storage area
AT+CMGR	Reads a message from a message storage area
AT+CMGS	Sends a short message from the device to entered tel. number
AT+CMGW	Writes a short message to SIM storage
AT+CMSS	Sends a message from SIM storage location value
AT+COPS?	Identifies the available mobile networks
AT+CPIN	Is used to query and enter a PIN code
AT+CPMS	Selects SMS memory storage types, to be used for short message operations
AT+CREG	Displays network registration status
AT+CSCA	Sets the short message service centre (SMSC) number
AT+CSCS	Selects the character set
AT+CSQ	Returns the signal strength of the registered network
AT+GMI	Returns the manufacturer specific identity
AT+GMM	Returns the manufacturer specific model identity
AT+GMR	Returns the manufacturer specific model revision identity
AT+GSN	Returns the product serial number
ATE	Determines whether or not the device echoes characters
ATI	Transmits the manufacturer specific information about the device

Table 58: List of AT commands

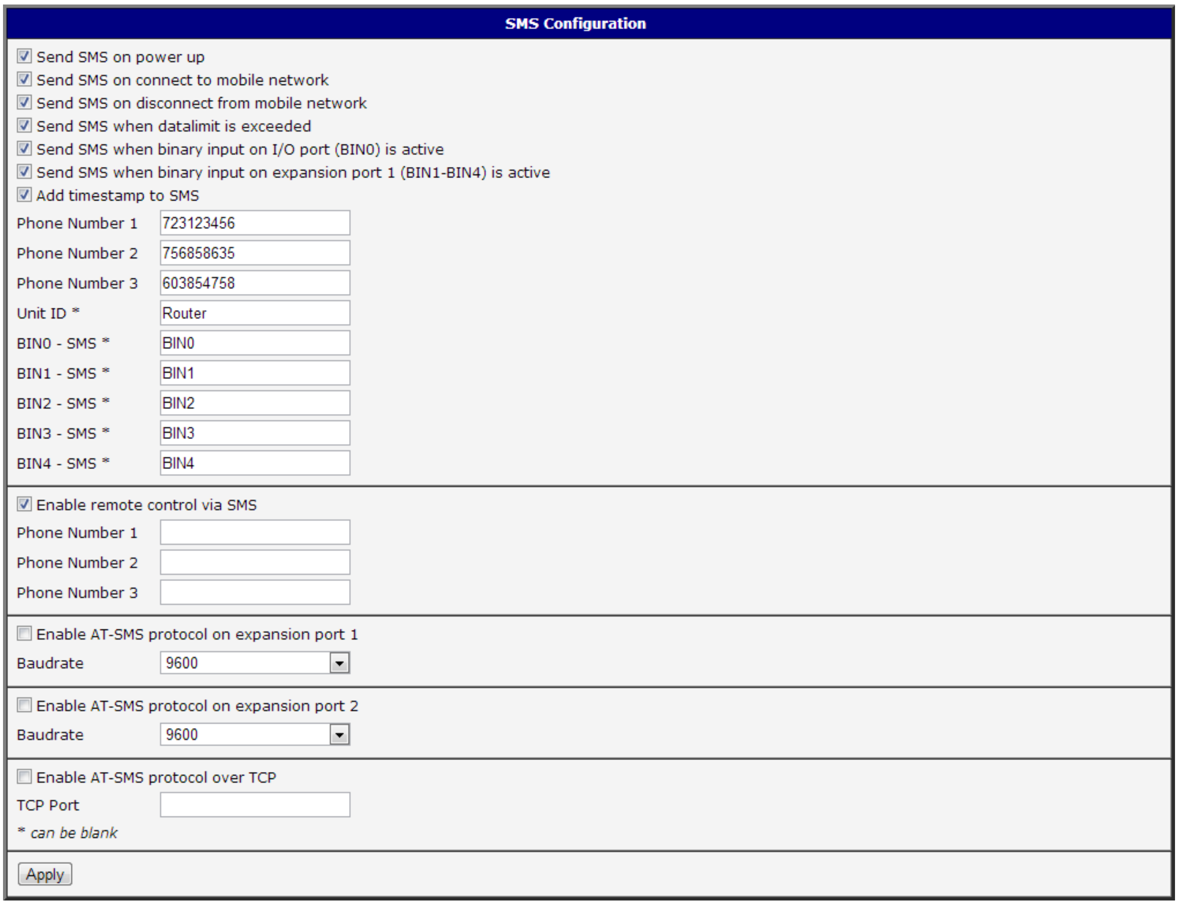
A detailed description and examples of these AT commands can be found in the application note *AT commands*.

After powering up the router, at the mentioned the phone number comes SMS in this form:
Router (Unit ID) has been powered up. Signal strength –xx dBm.

After connect to mobile network, at the mentioned phone number comes SMS in this form:
Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

After disconnect to mobile network, at the mentioned phone number comes SMS in this form:
Router (Unit ID) has lost connection to mobile network. IP address xxx.xxx.xxx.xxx

Configuration of sending this SMS is following:



SMS Configuration

☑ Send SMS on power up
☑ Send SMS on connect to mobile network
☑ Send SMS on disconnect from mobile network
☑ Send SMS when datalimit is exceeded
☑ Send SMS when binary input on I/O port (BIN0) is active
☑ Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
☑ Add timestamp to SMS

Phone Number 1: 723123456
Phone Number 2: 756858635
Phone Number 3: 603854758
Unit ID *: Router
BIN0 - SMS *: BIN0
BIN1 - SMS *: BIN1
BIN2 - SMS *: BIN2
BIN3 - SMS *: BIN3
BIN4 - SMS *: BIN4

☑ Enable remote control via SMS
Phone Number 1:
Phone Number 2:
Phone Number 3:

☐ Enable AT-SMS protocol on expansion port 1
Baudrate: 9600

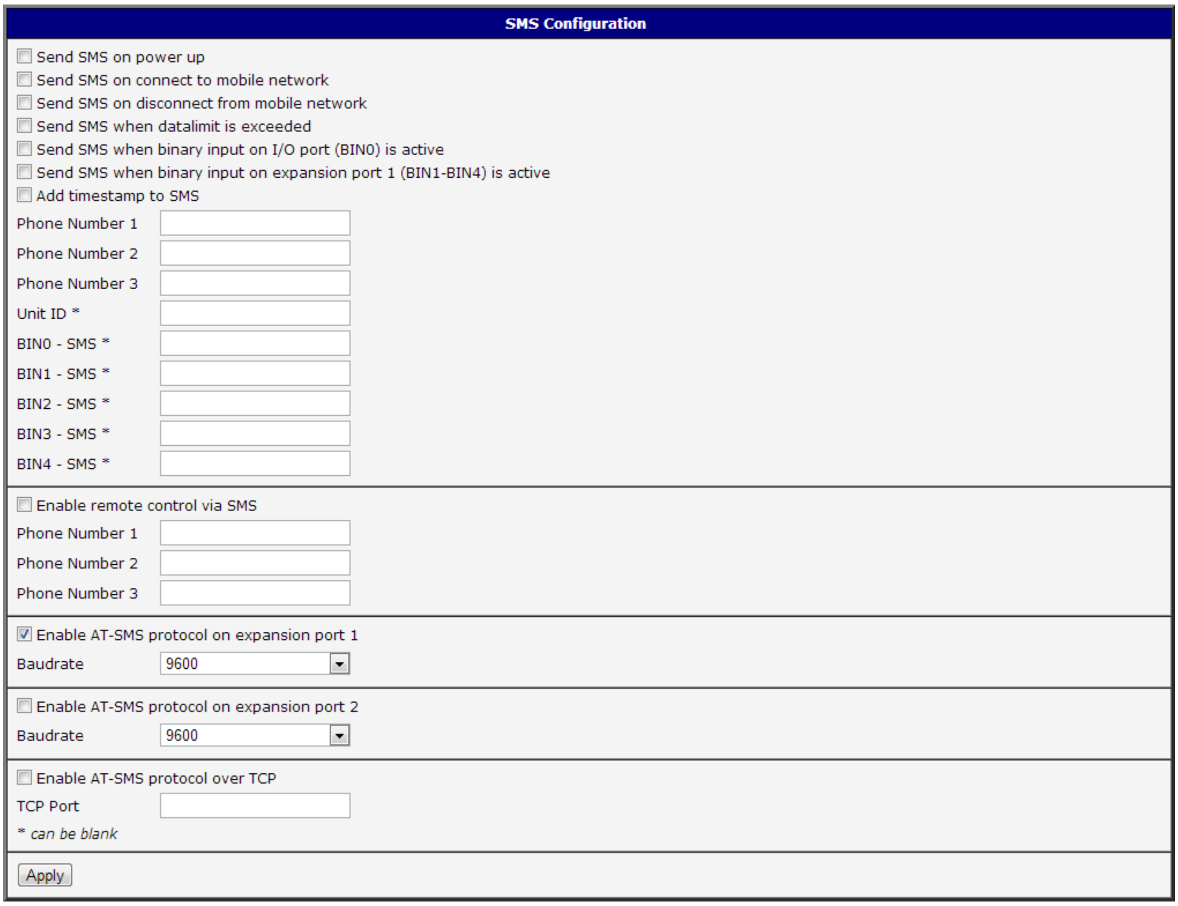
☐ Enable AT-SMS protocol on expansion port 2
Baudrate: 9600

☐ Enable AT-SMS protocol over TCP
TCP Port:

** can be blank*

Figure 48: Example of SMS configuration 1

Example of the router configuration for SMS sending via serial interface on the PORT1:



SMS Configuration

□ Send SMS on power up
□ Send SMS on connect to mobile network
□ Send SMS on disconnect from mobile network
□ Send SMS when datalimit is exceeded
□ Send SMS when binary input on I/O port (BIN0) is active
□ Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
□ Add timestamp to SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	
BIN1 - SMS *	
BIN2 - SMS *	
BIN3 - SMS *	
BIN4 - SMS *	

□ Enable remote control via SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	

☑ Enable AT-SMS protocol on expansion port 1

Baudrate 9600

□ Enable AT-SMS protocol on expansion port 2

Baudrate 9600

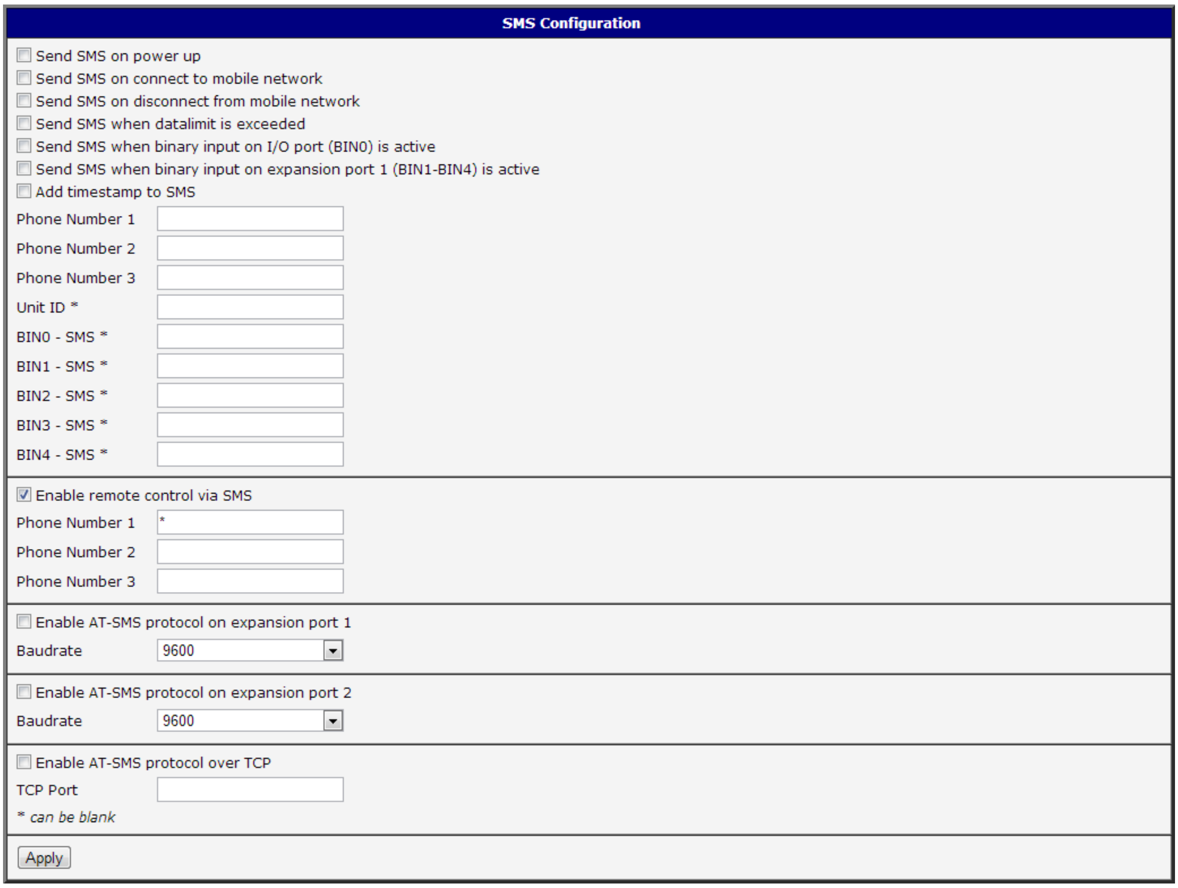
□ Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 49: Example of SMS configuration 2

Example of the router configuration for controlling via SMS from every phone numbers:



SMS Configuration

□ Send SMS on power up
□ Send SMS on connect to mobile network
□ Send SMS on disconnect from mobile network
□ Send SMS when datalimit is exceeded
□ Send SMS when binary input on I/O port (BIN0) is active
□ Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
□ Add timestamp to SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	
BIN1 - SMS *	
BIN2 - SMS *	
BIN3 - SMS *	
BIN4 - SMS *	

☑ Enable remote control via SMS

Phone Number 1	*
Phone Number 2	
Phone Number 3	

□ Enable AT-SMS protocol on expansion port 1

Baudrate	9600

□ Enable AT-SMS protocol on expansion port 2

Baudrate	9600

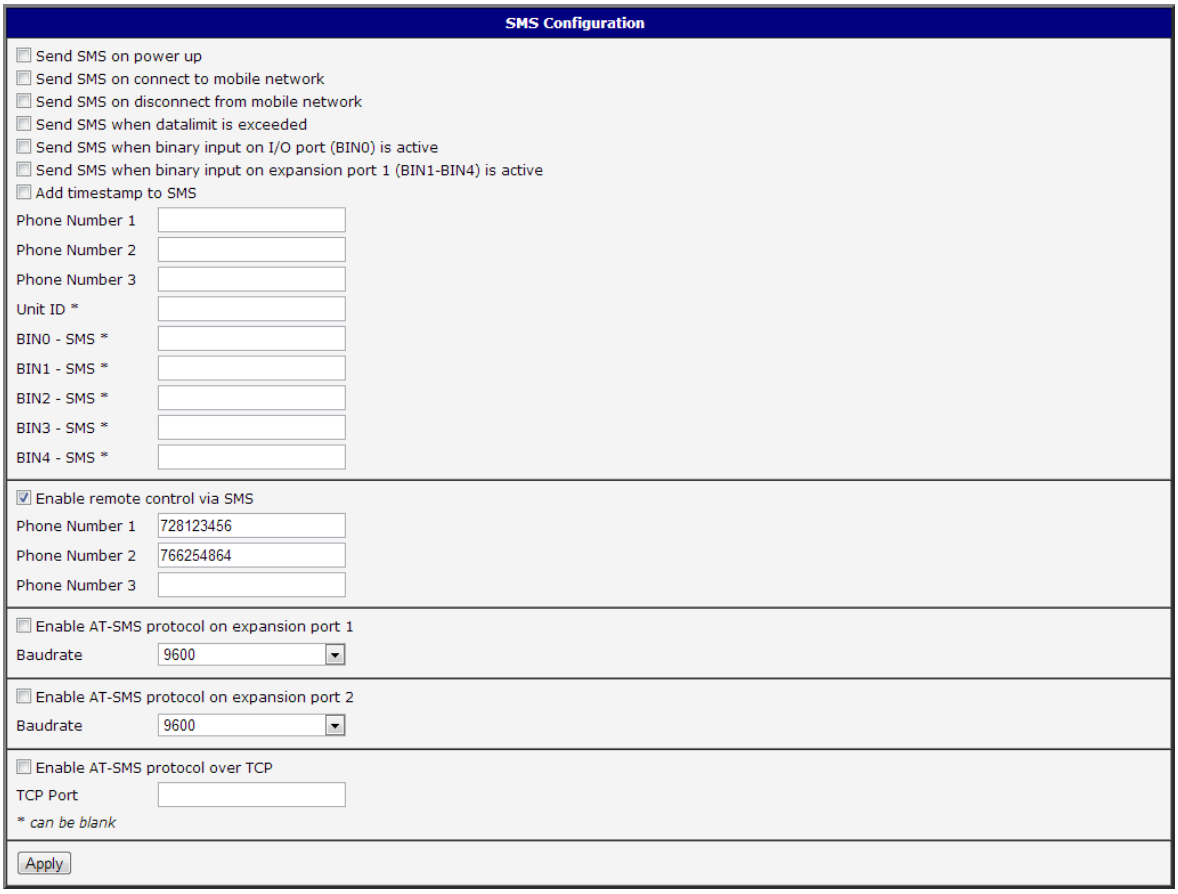
□ Enable AT-SMS protocol over TCP

TCP Port	

** can be blank*

Figure 50: Example of SMS configuration 3

Example of the router configuration for controlling via SMS from two phone numbers:



SMS Configuration

☐ Send SMS on power up
☐ Send SMS on connect to mobile network
☐ Send SMS on disconnect from mobile network
☐ Send SMS when datalimit is exceeded
☐ Send SMS when binary input on I/O port (BIN0) is active
☐ Send SMS when binary input on expansion port 1 (BIN1-BIN4) is active
☐ Add timestamp to SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	
Unit ID *	
BIN0 - SMS *	
BIN1 - SMS *	
BIN2 - SMS *	
BIN3 - SMS *	
BIN4 - SMS *	

☑ Enable remote control via SMS

Phone Number 1	728123456
Phone Number 2	766254864
Phone Number 3	

☐ Enable AT-SMS protocol on expansion port 1

Baudrate 9600

☐ Enable AT-SMS protocol on expansion port 2

Baudrate 9600

☐ Enable AT-SMS protocol over TCP

TCP Port

** can be blank*

Figure 51: Example of SMS configuration 4

1.26 Expansion port configuration

Configuring of the expansion ports PORT1 and PORT2 can cause selecting *Expansion Port 1* or *Expansion Port 2*.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit • none – Will be sent without parity. • even – Will be sent with even parity. • odd – Will be sent with odd parity.
Stop Bits	Number of stop bit.
Split Timeout	Time to rupture reports. If you receive will identify the gap between two characters, which is longer than the parameter value in milliseconds. Then all of the received data compiled and sent the message.
Protocol	Protocol: • TCP – communication using a linked protocol TCP • UDP – communication using a unlinked protocol UDP
Mode	Mode of connection: • TCP server – The router will listen to incoming requests about TCP connection. • TCP client – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	In mode TCP client it is necessary to enter the Server address and final TCP port.
TCP Port	In both modes of connection is necessary to specify the TCP port on which the router will communicate TCP connections.

Table 59: Expansion PORT configuration 1

After check *Check TCP connection*, it activates established of TCP connection.

Item	Description
Keepalive Time	Time, after which it will carry out verification of the connection
Keepalive Interval	Waiting time on answer
Keepalive Probes	Number of tests

Table 60: Expansion PORT configuration 2

When you select items *Use CD as indicator of the TCP connection* is activated function indication TCP connection using signal CD (DTR on the router).

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

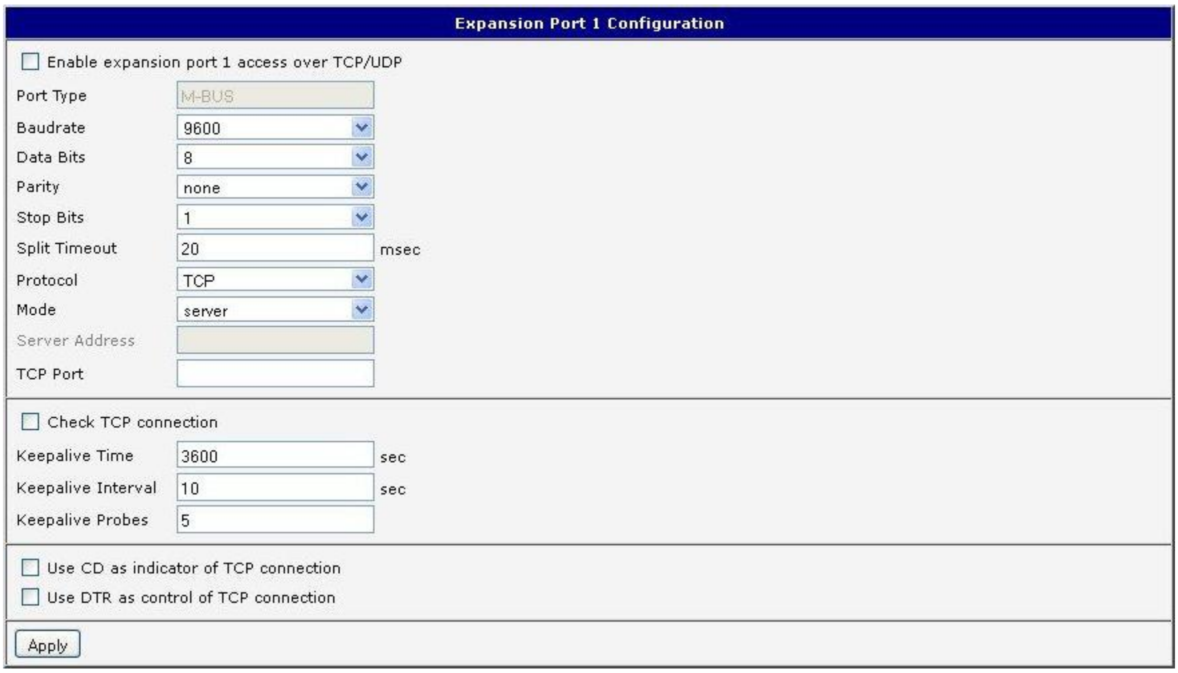
Table 61: CD signal description

When you select items *Use DTR as control of TCP connection* is activated function control TCP connection using signal DTR (CD on the router).

DTR	Description server	Description client
Active	The router allows establishing a TCP connection	Router starts TCP connection
Nonactive	The router does not permit establishing a TCP connection	Router stops TCP connection

Table 62: DTR signal description

The changes in settings will apply after pressing the *Apply* button.



Expansion Port 1 Configuration

☐ Enable expansion port 1 access over TCP/UDP

Port Type	M-BUS	
Baudrate	9600	
Data Bits	8	
Parity	none	
Stop Bits	1	
Split Timeout	20	msec
Protocol	TCP	
Mode	server	
Server Address		
TCP Port		

☐ Check TCP connection

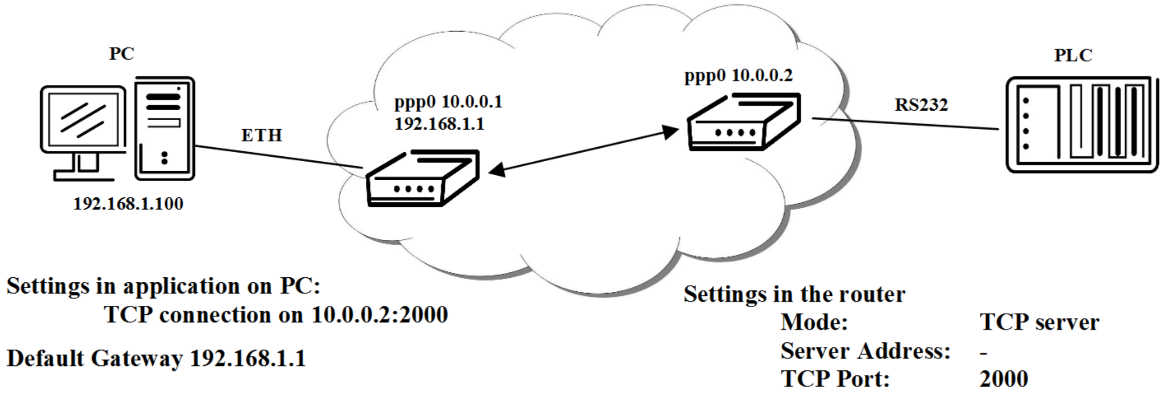
Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

☐ Use CD as indicator of TCP connection

☐ Use DTR as control of TCP connection

Figure 52: Expansion port configuration

Example of external port configuration:



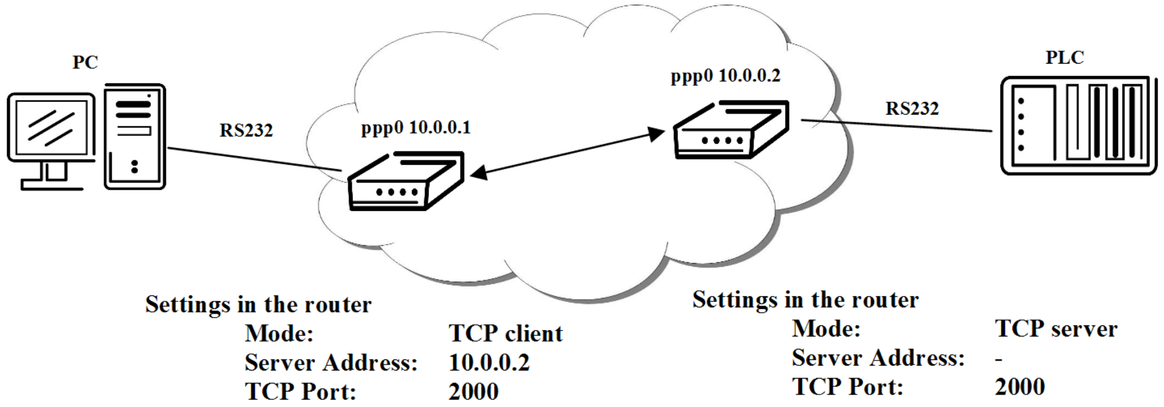
Settings in application on PC:
TCP connection on 10.0.0.2:2000

Default Gateway 192.168.1.1

Settings in the router

Mode:	TCP server
Server Address:	-
TCP Port:	2000

Figure 53: Example of expansion port configuration 1



Settings in the router

Mode:	TCP client
Server Address:	10.0.0.2
TCP Port:	2000

Settings in the router

Mode:	TCP server
Server Address:	-
TCP Port:	2000

Figure 54: Example of expansion port configuration 2

1.27 USB port configuration

The USB port configuration can be called up by airbrush option *USB Port* in menu. Configuration can be done, if we have USB/RS232 converter.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit • none – Will be sent without parity. • even – Will be sent with even parity. • odd – Will be sent with odd parity.
Stop Bits	Number of stop bit.
Split Timeout	Time to rupture reports. If you receive will identify the gap between two characters, which is longer than the parameter value in milliseconds. Then all of the received data compiled and sent the message.
Protocol	Communication protocol: • TCP – communication using a linked protocol TCP • UDP – communication using a unlinked protocol UDP
Mode	Mode of connection: • TCP server – The router will listen to incoming requests about TCP connection. • TCP client – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	In mode TCP client it is necessary to enter the Server address and final TCP port.
TCP Port	In both modes of connection is necessary to specify the TCP port on which the router will communicate TCP connections.

Table 63: USB port configuration 1

After check *Check TCP connection*, it activates verification of established TCP connection.

Item	Description
Keepalive Time	Time, after which it will carry out verification of the connection
Keepalive Interval	Waiting time on answer
Keepalive Probes	Number of tests

Table 64: USB PORT configuration 2

When you select items *Use CD as indicator of the TCP connection* is activated function indication TCP connection using signal CD (DTR on the router).

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

Table 65: CD signal description

When you select items *Use DTR as control of TCP connection* is activated function control TCP connection using signal DTR (CD on the router).

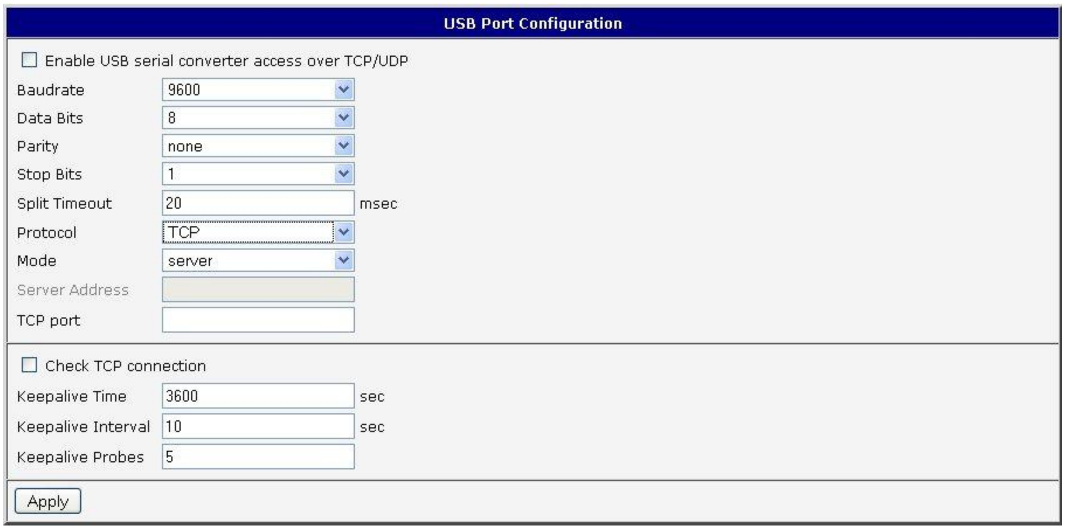
DTR	Description server	Description client
Active	The router allows establishing a TCP connection	Router starts TCP connection
Nonactive	The router does not permit establishing a TCP connection	Router stops TCP connection

Table 66: DTR signal description

Supported USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×(supported from firmware version 3.0.1)

The changes in settings will apply after pressing the *Apply* button



USB Port Configuration

☐ Enable USB serial converter access over TCP/UDP

Baudrate	9600	
Data Bits	8	
Parity	none	
Stop Bits	1	
Split Timeout	20	msec
Protocol	TCP	
Mode	server	
Server Address		
TCP port		

☐ Check TCP connection

Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

Figure 55: USB configuration

Example of USB port configuration:

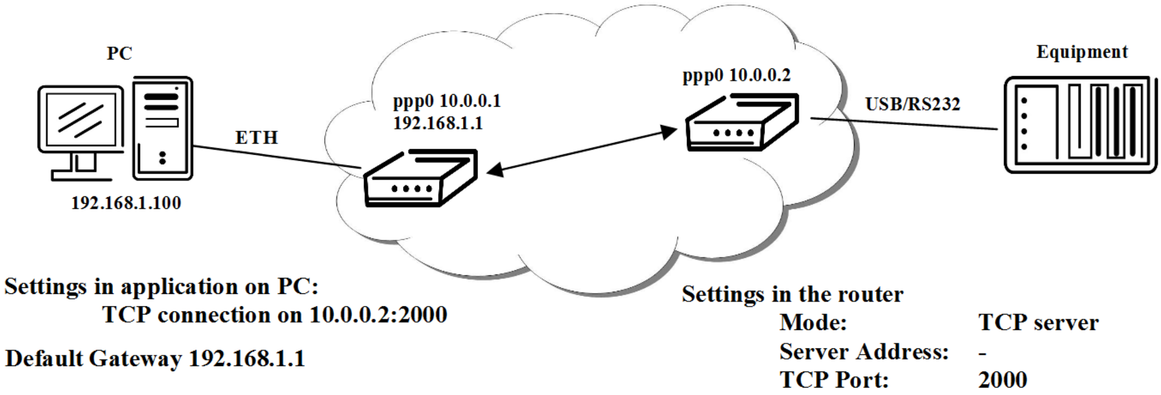


Figure 56: Example of USB port configuration 1

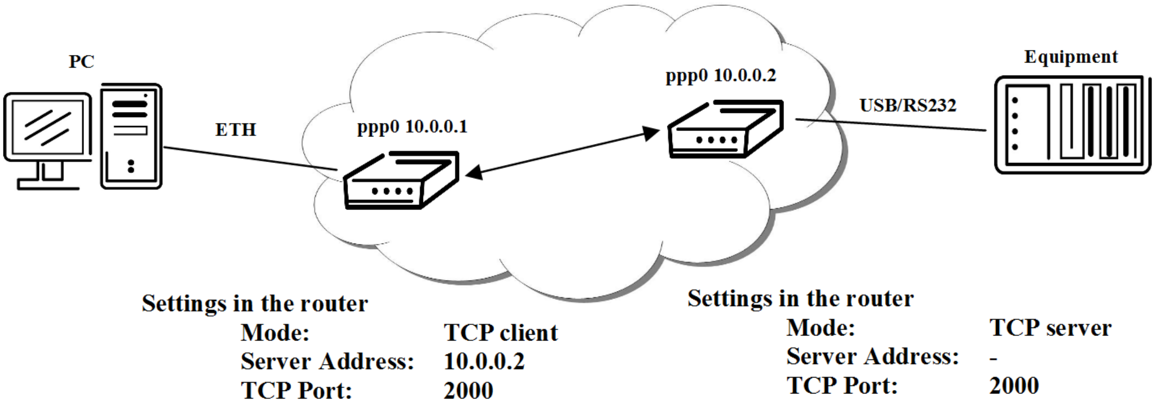
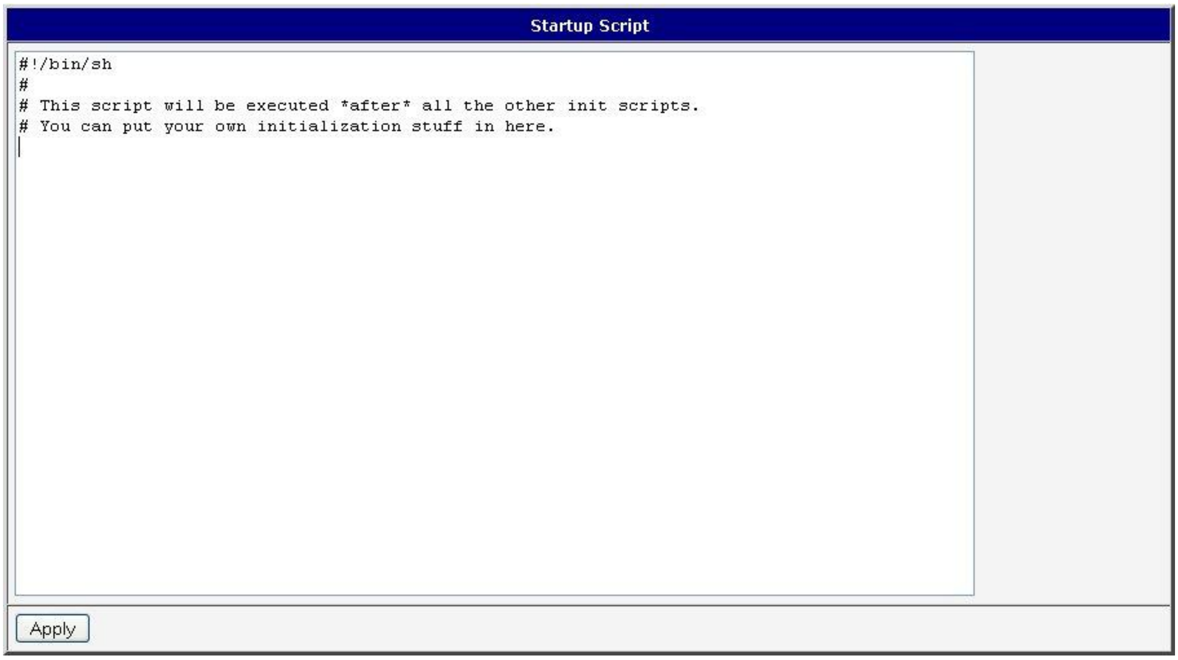


Figure 57: Example of USB port configuration 2

1.28 Startup script

In the window *Startup Script* it is possible to create own scripts which will be executed after all initial scripts.

The changes in settings will apply after pressing the *Apply* button.

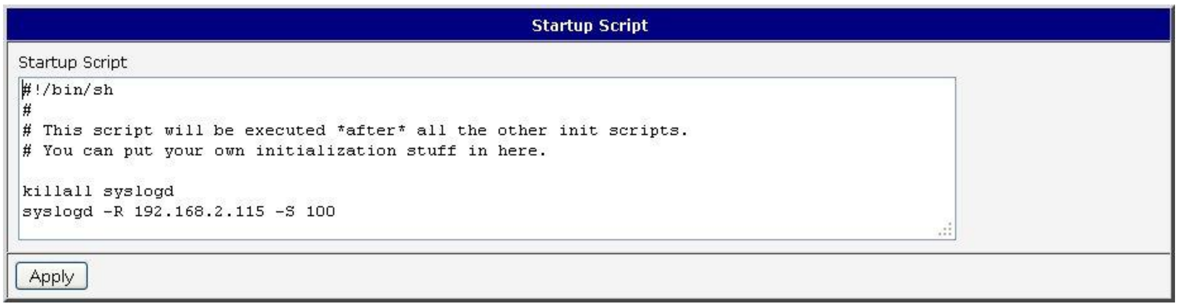


```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.
```

Figure 58: Startup script

Change take effect after shut down and witch on router by the help of button Reboot in web administration or by SMS message.

Example of Startup script: When start the router, stop syslogd program and start syslogd with remote logging on address 192.168.2.115 and limited to 100 entries listing.



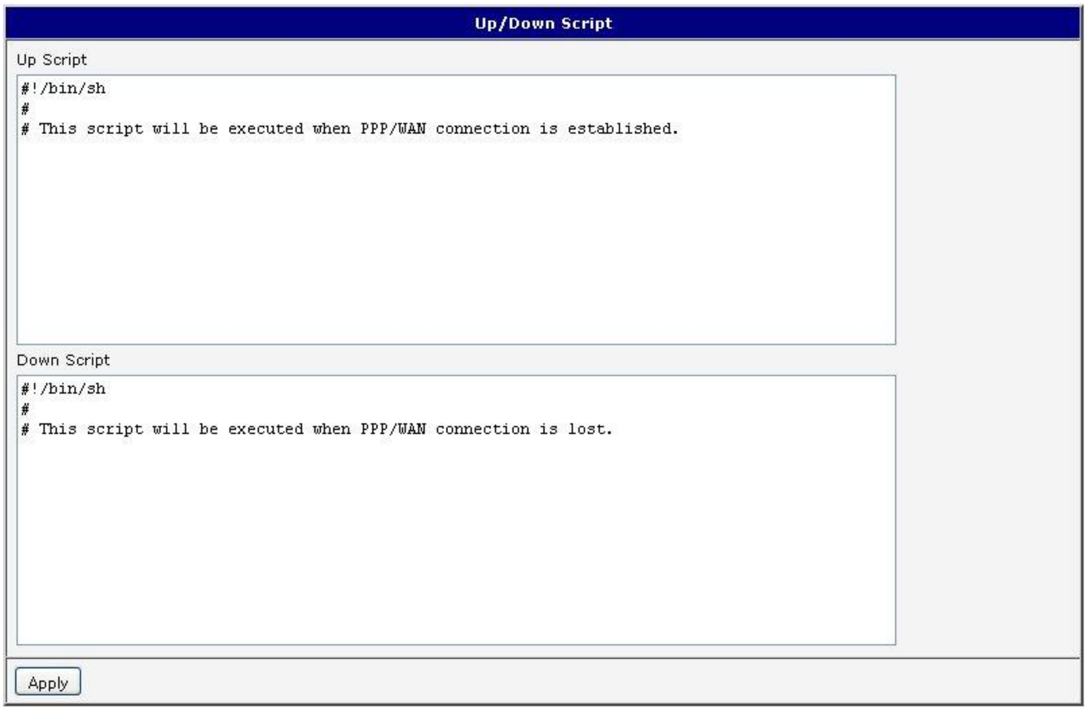
```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

killall syslogd
syslogd -R 192.168.2.115 -S 100
```

Figure 59: Example of Startup script

1.29 Up/Down script

In the window *Up/Down Script* it is possible to create own scripts. In the item *Up script* is defined scripts, which begins after establishing a PPP/WAN connection. In the item *Down Script* is defines script, which begins after lost a PPP/WAN connection.

The changes in settings will apply after pressing the *Apply* button.



Up/Down Script

Up Script

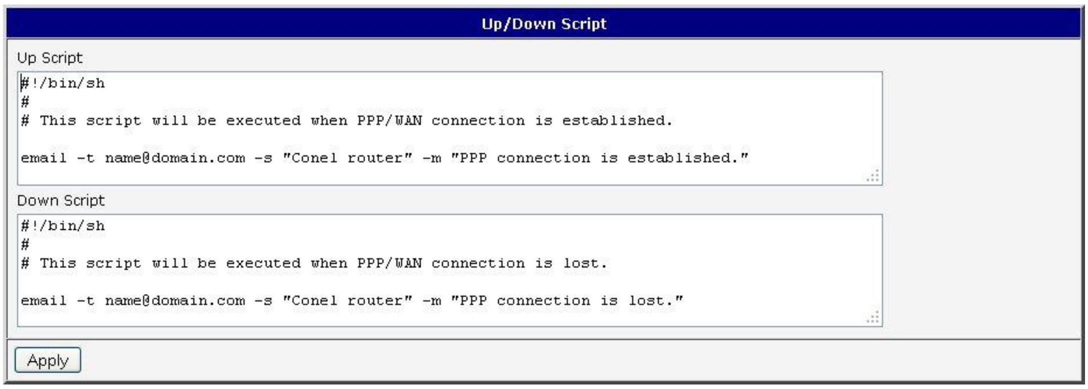
```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is established.
```

Down Script

```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is lost.
```

Figure 60: Up/Down script

Example of UP/Down script: After establishing or lost a connection, the router sends an email with information about establishing or loss a connection.



Up/Down Script

Up Script

```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is established.

email -t name@domain.com -s "Conel router" -m "PPP connection is established."
```

Down Script

```
#!/bin/sh
#
# This script will be executed when PPP/WAN connection is lost.

email -t name@domain.com -s "Conel router" -m "PPP connection is lost."
```

Figure 61: Example of Up/Down script

1.30 Automatic update configuration

In the window *Automatic update* it is possible to set automatic configuration update. This choice enables that the router automatically downloads the configuration and the newest firmware from the server itself. The configuration and firmware are stores on the server.

By *Enable automatic update of configuration* it is possible to enable automatic configuration update and by *Enable automatic update of firmware* it is possible to enable firmware update.

Item	Description
Source	In the item source can be set, where new firmware download: • HTTP/FTP server – new firmware or configuration look at address in the Base URL item. • USB flash drive – Router finds current firmware or configuration in the root directory of the connected USB device. • Both – looking for the current firmware or configuration from both sources.
Base URL	By parameter Base URL it is possible to enter base part of the domain or IP address, from which the configuration file will be downloaded.
Unit ID	Name of configuration. If the Unit ID is not filled, then as the file name used the MAC address of the router. (The delimiter is a colon is used instead of a dot.)
Update Hour	Automatic configuration update starts 5 minutes after turning on the router and then every 24 hours or it is possible to set the time of automatic configuration in parameter Update Hour. If the entered URL is different configuration than in the router then the router downloads this configuration and restarts itself.

Table 67: Automatic update configuration

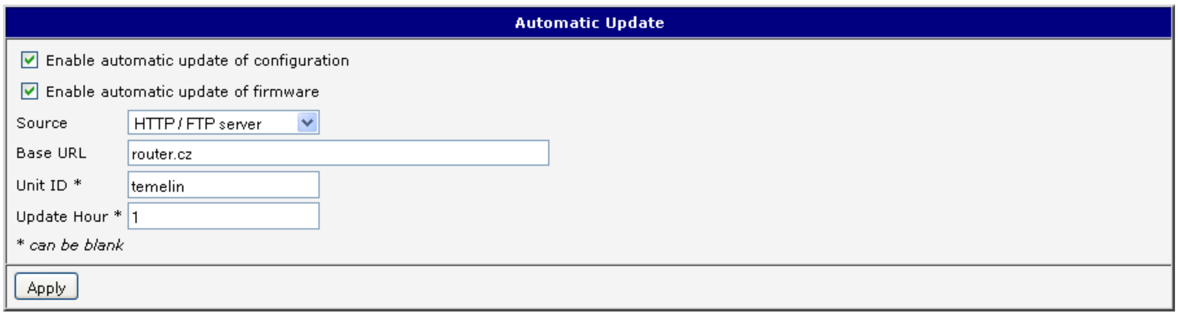
The *configuration file* name is from parameter *Base URL*, hardware MAC address of ETH0 interface and *cfg* extension. Hardware MAC address and *cfg* extension is connected automatically and it isn't needed to enter this. By parameter *Unit ID* enabled it defines the concrete configuration name which will be download to the router. When using parameter *Unit ID*, hardware MAC address in configuration name will not be used.

The *firmware file* name is from parameter *Base URL*, type of router and bin extension.

It is necessary to load two files (.bin and .ver) to the HTTP/FTP server. If there is uploaded only the .bin file and the HTTP server send wrong answer *200 OK* (instead of expected *404 Not Found*) when the device try to download the nonexistent .ver file, then there is a high risk that the router will download the .bin file over and over again.

The following examples find if there is a new firmware or configuration each day at 1:00 in the morning. An example is given on the type of router ER75i v2.

- Firmware: http://router.cz/er75i-v2.bin
- Configuration file: http://router.cz/temelin.cfg



Automatic Update

☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

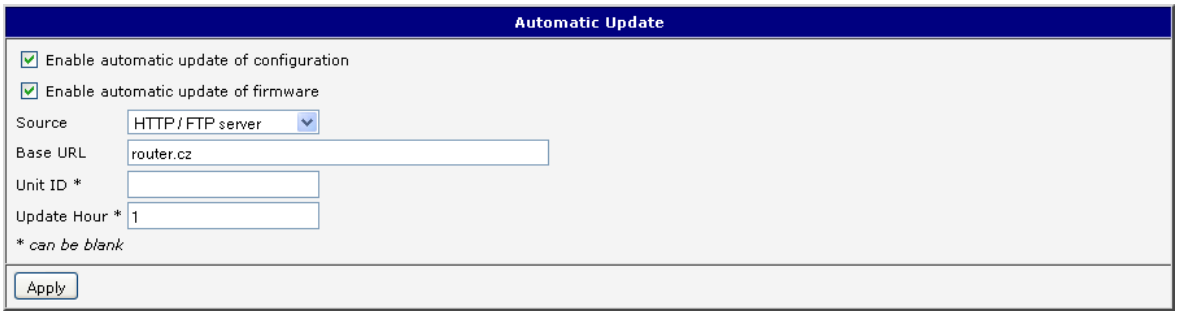
Source	HTTP / FTP server
Base URL	router.cz
Unit ID *	temelin
Update Hour *	1

* can be blank

Figure 62: Example of automatic update 1

The following examples find if there is a new firmware or configuration each day at 1:00 in the morning. An example is given on the type of router ER75i v2 with MAC address 00:11:22:33:44:55.

- Firmware: http://router.cz/er75i-v2.bin
- Configuration file: http://router.cz/00.11.22.33.44.55.cfg



Automatic Update

☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

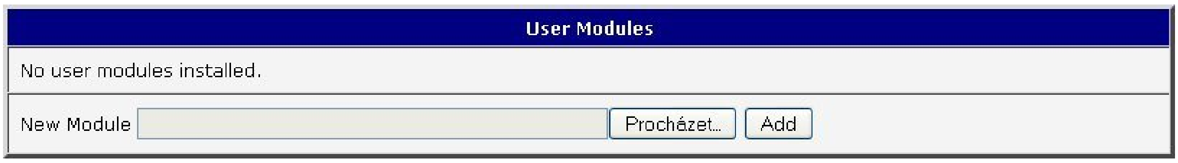
Source	HTTP / FTP server
Base URL	router.cz
Unit ID *	
Update Hour *	1

* can be blank

Figure 63: Example of automatic update 2

1.31 User modules

Configuration of user modules can be accessed by selecting the *User Modules* item. It is possible to add new modules, delete them or switch to their configuration. Use the *Browse* button to select the user module (compiled module has tgz extension). The module is added using the *Add* button.



User Modules

No user modules installed.

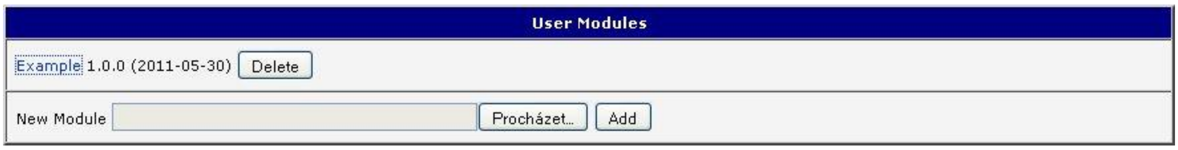
New Module

Figure 64: User modules

Added module appears in the list of modules on the same page. If the module contains index.html or index.cgi page, module name serves as a link to this page. The module can be deleted using the *Delete* button.

Updating of the module can be done in the same way like adding a new module. Module with a higher (newer) version will replace the existing module. The current module configuration is kept in same state.

Programming and compiling of modules are described in the programming guide.



User Modules

Example 1.0.0 (2011-05-30)

New Module

Figure 65: Added user module

There are for example these user's modules:

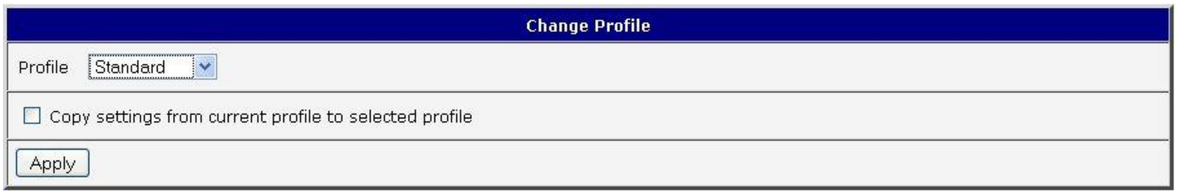
Module name	Description
MODBUS TCP2RTU	Provides a conversion of MODBUS TCP/IP protocol to MDBUS RTU protocol, which can be operated on the serial line.
Easy VPN client	Provides secure connection of LAN network behind our router with LAN network behind CISCO router.
NMAP	Allows to do TCP and UDP scan.
Daily Reboot	Allows to perform daily reboot of the router at the specified time.
HTTP Authentication	Adds the process of authentication to a server that doesn't provide this service.
BGP, RIP, OSPF	Add support of dynamic protocols.
PIM SM	Adds support of multicast routing protocol PIM-SM.
WMBUS Concentrator	Allows to receive messages from WMBUS meters and saves contents of these messages to XML file.
pduSMS	Sends short messages (SMS) to specified number.
GPS	Allows v2 router to provide location and time information in all weather, anywhere on or near the Earth, where there is an unobstructed line of sight to four or more GPS satellites.
Pinger	Allows to manually or automatically verify the functionallity of the connection between two network interfaces (ping).
WiFi STA	Allows router to behave as a classical WiFi client station.
IS-IS	Add support of IS-IS protocol.

Table 68: User modules

1.32 Change profile

To open the dialog box for changing profile select the *Change Profile* menu item. Profile switch is making by press the button *Apply*. Change take effect after restarting router by the help of button *Reboot* in web administration or by SMS message. It is possible select the standard profile or up to three alternative profiles. It is possible to copy actual configuration to selected configuration by selecting *Copy settings from current profile to selected profile*.

Example of usage profiles: Profiles can be used for example to switch between different modes of operation of the router (router has compiled a connection, the router has not compiled a connection and the router creates a tunnel to the service center). Change the profile can then be done using a binary input, SMS or Web interface of the router.


Change Profile

Profile: Standard

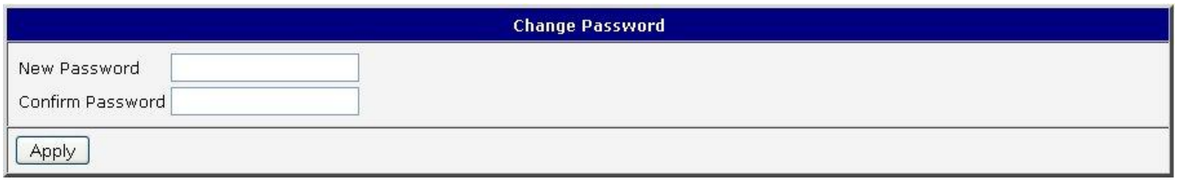
□ Copy settings from current profile to selected profile

Figure 66: Change profile

1.33 Change password

To open the dialog box for changing the access password select the *Change Password* menu item. The new password will be saved after pressing the *Apply* button.

In basic settings of the router the password is set on default form *root*. For higher security of your network we recommend changing this password.

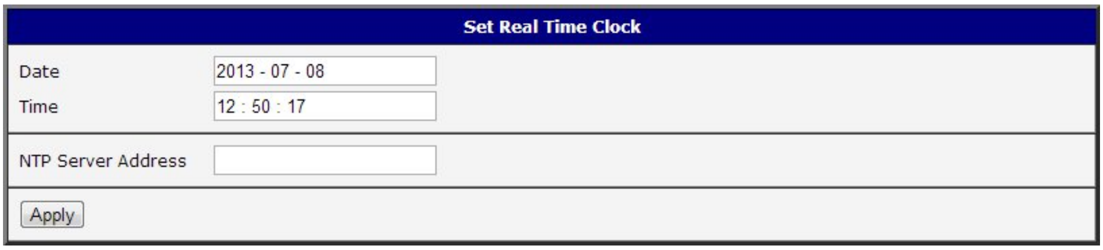

Change Password

New Password:
Confirm Password:

Figure 67: Change password

1.34 Set real time clock

Disposable setting of the router internal clock can be invoked by pressing the *Set Real Time Clock* item in the main menu of the web interface. Date and time can be set manually through the *Date* and *Time* items. Always enter data in a format that is illustrated in the figure below. The clock can be also adjusted according to the specified NTP server. Finally, it is necessary to press the *Apply* button.



Set Real Time Clock

Date 2013 - 07 - 08

Time 12 : 50 : 17

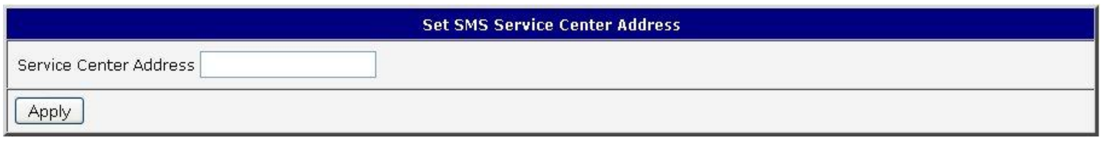
NTP Server Address

Figure 68: Set real time clock

1.35 Set SMS service center address

For industrial router XR5i v2 is not available Set SMS service center address item.

In some cases it is needed to set the phone number of the SMS service centre because of SMS sending. This parameter can not be set when the SIM card has set phone number of the SMS service centre. The phone number can be formed without international prefix xxx xxx xxx or with international prefix for example +420 xxx xxx xxx.



Set SMS Service Center Address

Service Center Address

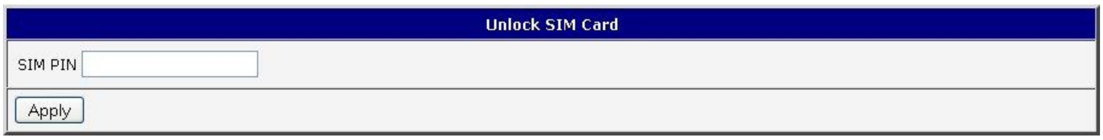
Figure 69: Set SMS service center address

1.36 Unlock SIM card

For industrial router XR5i v2 is not available Unlock SIM card item.

Possibility to unlock SIM PIN is under *Unlock SIM Card* item. If the inserted SIM card is secured by a PIN number, enter the PIN to field *SIM PIN* and push-button *Apply*.

SIM card is blocked after three failed attempts to enter the PIN code.



Unlock SIM Card

SIM PIN

Figure 70: Unlock SIM card

1.37 Send SMS

For industrial router XR5i v2 is not available Send SMS item.

Sending SMS messages is possible in menu *Send SMS*. The SMS message will be sent after entering the *Phone number* and text SMS (*Message*) and by pushing button *Send*.

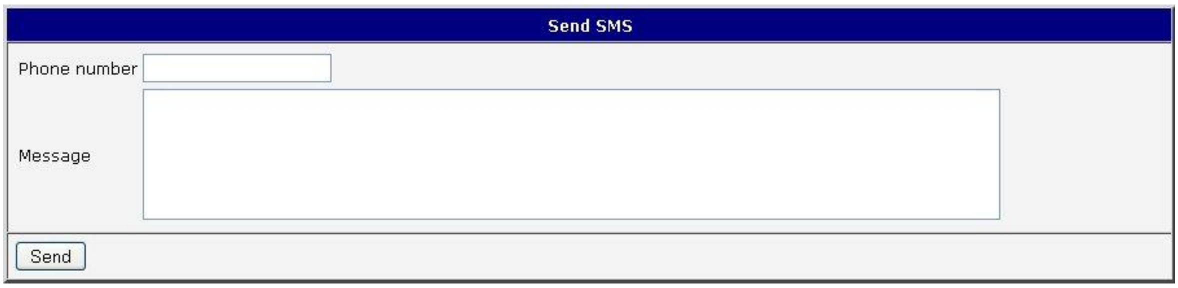


Figure 71: Send SMS

SMS message sending via HTTP request is in the form:

GET/send_exec.cgi?phone=%2B420712345678&message=Test HTTP/1.1
Authorization: Basic cm9vdDpyb290

HTTP request will be sent to TCP connection on router port 80. Router sends an SMS message with text *"Test"*. SMS is sent to phone number *"420712345678"*. Authorization is in the format "user:password" coded by BASE64. In the example is used for root:root.

1.38 Backup configuration

The router configuration is possible to save by help of the *Backup Configuration* menu item. After clicking on this menu it is possible to check a destination directory, where it will save the router configuration.

1.39 Restore configuration

In case it is needed to restore the router configuration, it is possible in *Restore Configuration* menu item to check configuration by help *Browse* button.

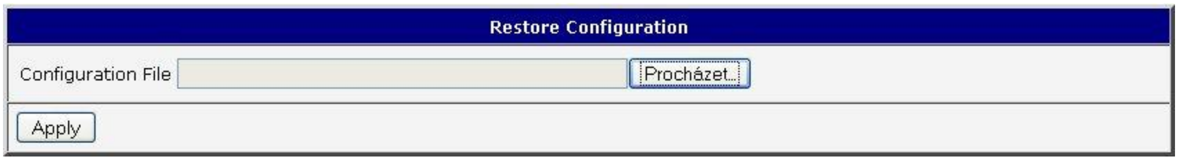
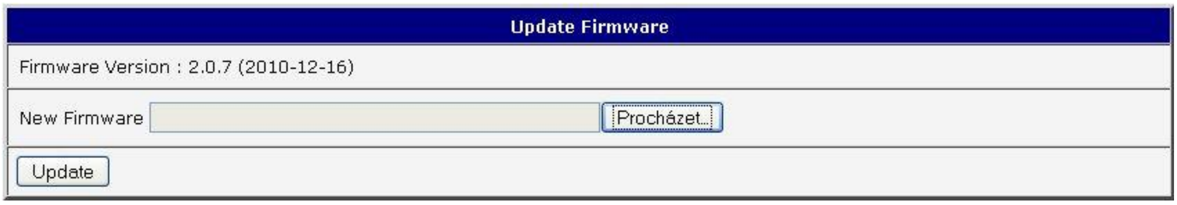


Figure 72: Restore configuration

1.40 Update firmware

To view the information about the firmware version and instructions for its update select the *Update Firmware* menu item. New firmware is selected via Browse button and update the following pressing the Update button.



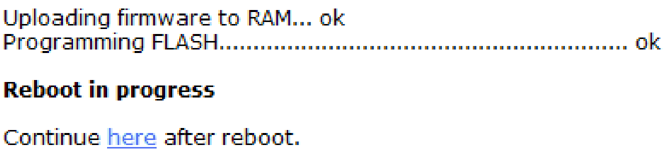
Update Firmware

Firmware Version : 2.0.7 (2010-12-16)

New Firmware

Figure 73: Update firmware

After successful firmware updating the following statement is listed:



```
Uploading firmware to RAM... ok
Programming FLASH............................................................ ok
```

Reboot in progress

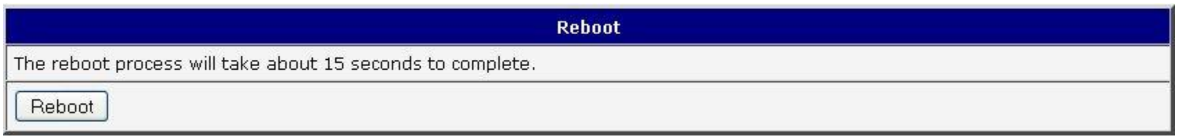
Continue here after reboot.

There is information about updating of the FLASH memory.

Upload firmware of different device can cause damage of the router!
During updating of the firmware permanent power supply has to be maintained.

1.41 Reboot

To reboot the router select the *Reboot* menu item and then press the *Reboot* button.



Reboot

The reboot process will take about 15 seconds to complete.

Figure 74: Reboot

2. Configuration setting over Telnet

Attention! If the SIM card isn't inserted in the router, it is impossible for the router to operate. The Included SIM card must be activated for GPRS transmissions.

Monitoring of status, configuration and administration of the router can be performed by means of the Telnet interface. After IP address entry to the Telnet it is possible to configure the router by the help of commands. The default IP address of the modem is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

For Telnet exists the following commands:

Command	Description
cat	file contain write
cp	copy of file
date	show/change of system time
df	displaying of informations about file system
dmesg	displaying of kernel diagnostics messages
echo	string write
email	Email send
free	displaying of informations about memory
gsmat	AT commend send
gsminfo	displaying of informations about signal quality
gsmsms	SMS send
hwclock	displaying/change of time in RTC
ifconfig	displaying/change of interface configuration
io	reading/writing input/output pins
ip	displaying/change of route table
iptables	displaying/modification of NetFilter rules
kill	process kill
killall	processes kill
ln	link create
ls	dump of directory contain
mkdir	file create
mv	file move
ntpdate	synchronization of system time with NTP server

Continued on next page

Continued from previous page

Command	Description
passwd	password change
ping	ICMP ping
ps	displaying of processes information
pwd	dump of actual directory
reboot	reboot
rm	file delete
rmdir	directory delete
route	displaying/change of route table
service	start/stop of service
sleep	pause on set seconds number
slog	displaying of system log
tail	displaying of file end
tcpdump	monitoring of network
touch	file create/actualization of file time stamp
vi	text editor

Table 69: Telnet commands